

# LINKSYS®

A Division of Cisco Systems, Inc.



2,4 GHz

## Wireless-N

### ADSL2+ Gateway

# User Guide

WIRELESS

Model No. **WAG300N (EU/LA)**

CISCO SYSTEMS



## Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2006 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

## How to Use this Guide

Your Guide to the Wireless-N ADSL2+ Gateway has been designed to make understanding networking with the Gateway easier than ever. Look for the following items when reading this User Guide:



This checkmark means there is a Note of interest and is something you should pay special attention to while using the Gateway.



This exclamation point means there is a Caution or Warning and is something that could damage your property or the Gateway.



This question mark provides you with a reminder about something you might need to do while using the Gateway.

In addition to these symbols, there are definitions for technical terms that are presented like this:

***word: definition.***

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

### **Figure 0-1: Sample Figure Description**

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

# Table of Contents

<b>Chapter 1: Introduction</b>	<b>1</b>
Welcome	1
What's in this User Guide?	2
<b>Chapter 2: Planning Your Network</b>	<b>4</b>
The Gateway's Functions	4
IP Addresses	4
<b>Chapter 3: Getting to Know the Wireless-N ADSL2+ Gateway</b>	<b>6</b>
Ports and Reset Button on Side Panel	6
LEDs on Side Panel	7
<b>Chapter 4: Connecting the Wireless-N ADSL2+ Gateway</b>	<b>8</b>
Overview	8
Wired Connection to a Computer	8
Wireless Connection to a Computer	9
<b>Chapter 5: Configuring the Wireless-N ADSL2+ Gateway</b>	<b>10</b>
Overview	10
How to Access the Web-based Utility	12
The Setup Tab	12
The Wireless Tab	21
The Security Tab	29
The Access Restrictions Tab	31
The Applications and Gaming Tab	33
The Administration Tab	40
The Status Tab	46
<b>Appendix A: Troubleshooting</b>	<b>50</b>
Common Problems and Solutions	50
Frequently Asked Questions	58
<b>Appendix B: Wireless Security</b>	<b>65</b>
Security Precautions	65
Security Threats Facing Wireless Networks	65
<b>Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter</b>	<b>68</b>
Windows 98 or Me Instructions	68
Windows 2000 or XP Instructions	69

<b>Appendix D: Upgrading Firmware</b>	<b>70</b>
<b>Appendix E: Glossary</b>	<b>71</b>
<b>Appendix F: Specifications</b>	<b>76</b>
<b>Appendix G: Warranty Information</b>	<b>78</b>
<b>Appendix H: Regulatory Information</b>	<b>79</b>
<b>Appendix I: Contact Information</b>	<b>91</b>

# List of Figures

Figure 2-1: Network	4
Figure 3-1: Ports and Reset Button on Side Panel	6
Figure 3-2: LEDs on Side Panel	7
Figure 4-1: Connect the ADSL Line	8
Figure 4-2: Connect a PC	8
Figure 4-3: Connect the Power	8
Figure 4-4: Connect the ADSL Line	9
Figure 4-5: Connect the Power	9
Figure 5-1: Basic Setup	12
Figure 5-2: RFC 1483 Bridged	13
Figure 5-3: RFC 1483 Routed	14
Figure 5-4: IPoA	14
Figure 5-5: RFC 2516 PPPoE	15
Figure 5-6: RFC 2364 PPPoA	15
Figure 5-7: Bridge Mode Only	16
Figure 5-8: Optional Settings	16
Figure 5-9: DDNS - DynDNS.org	18
Figure 5-10: DDNS - TZ0.com	18
Figure 5-11: Advanced Routing	19
Figure 5-12: Routing Table	20
Figure 5-13: Basic Wireless Settings	21
Figure 5-14: Wireless Security - PSK-Personal	22
Figure 5-15: Wireless Security - PSK2-Personal	22
Figure 5-16: Wireless Security - PSK-Enterprise	23
Figure 5-17: Wireless Security - PSK2-Enterprise	23
Figure 5-18: Wireless Security - RADIUS	24
Figure 5-19: Wireless Security - WEP	25
Figure 5-20: Wireless MAC Filter	26
Figure 5-21: Wireless Client List	26
Figure 5-22: Advanced Wireless Settings	27
Figure 5-23: Firewall	29
Figure 5-24: VPN Passthrough	30

Figure 5-25: Internet Access Policy	31
Figure 5-26: Internet Policy Summary	31
Figure 5-27: List of PCs	32
Figure 5-28: Single Port Forwarding	33
Figure 5-29: Port Range Forwarding	34
Figure 5-30: Port Triggering	35
Figure 5-31: DMZ	36
Figure 5-32: QoS	37
Figure 5-33: QoS - Online Game	38
Figure 5-34: QoS - MSN Messenger	38
Figure 5-35: QoS - YAHOO Messenger	38
Figure 5-36: QoS - Skype	38
Figure 5-37: QoS - Voice Device	38
Figure 5-38: QoS - Add a New Application (Port Range)	38
Figure 5-39: QoS - Add a New Application (MAC Address)	39
Figure 5-40: Management	40
Figure 5-41: Reporting	42
Figure 5-42: View Log	42
Figure 5-43: Diagnostics	43
Figure 5-44: Ping Test	43
Figure 5-45: Backup & Restore	44
Figure 5-46: Factory Defaults	45
Figure 5-47: Firmware Upgrade	45
Figure 5-48: Gateway	46
Figure 5-49: Local Network	47
Figure 5-50: DHCP Active IP Table	47
Figure 5-51: ARP/RARP Table	47
Figure 5-52: Wireless	48
Figure 5-53: DSL Connection	49
Figure C-1: IP Configuration Screen	68
Figure C-2: MAC Address/Adapter Address	68
Figure C-3: MAC Address/Physical Address	69
Figure D-1: Firmware Upgrade	70

# Chapter 1: Introduction

## Welcome

Thank you for choosing the Wireless-N ADSL2+ Gateway. The Gateway will allow you to network wirelessly better than ever, sharing Internet access, files and fun, easily and securely and with a greater range of up to three times farther than standard Wireless-G.

The incredible speed of Wireless-N makes it ideal for media-centric applications like streaming video and Voice over IP (VoIP) telephony, so your network can handle multiple data streams at the same time, with no degradation in performance.

How does the Gateway do all of this? By connecting the Internet, as well as your computers and peripherals, to the Gateway, then the Gateway can direct and control communications for your network. Plus, since the Gateway is wireless, Internet access can be shared over the wireless broadcast as well as the wired network.

Use wireless security to secure your wireless network while the whole network is protected through a Stateful Packet Inspection (SPI) firewall and Network Address Translation (NAT) technology. The Gateway also offers VPN passthrough and other features, which can be configured through the easy-to-use, browser-based utility.

But what does all of this mean?

Networks are useful tools for sharing Internet access and computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks not only are useful in homes and offices, but also can be fun.

PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called "wired". PCs equipped with wireless cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wireless Local Area Network. Since the Gateway has wireless capabilities, it can bridge your wired and wireless networks, letting them communicate with each other.

Linksys recommends using the Setup CD-ROM for first-time installation of the Gateway. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then use the instructions in this Guide to help you connect the Gateway, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Wireless-N ADSL2+ Gateway.

**802.11g:** an IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

**spi (stateful packet inspection) firewall:** a technology that inspects incoming packets of information before allowing them to enter the network.

**firewall:** Security measures that protect the resources of a local network from intruders.

**nat (network address translation):** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

**network:** a series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users

**lan (local area network):** The computers and networking products that make up the network in your home or office.

## What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-N ADSL2+ Gateway.

- **Chapter 1: Introduction**  
This chapter describes applications of the Wireless-N ADSL2+ Gateway and this User Guide.
- **Chapter 2: Planning Your Network**  
This chapter describes the basics of networking.
- **Chapter 3: Getting to Know the Wireless-N ADSL2+ Gateway**  
This chapter describes the physical features of the Gateway.
- **Chapter 4: Connecting the Wireless-N ADSL2+ Gateway**  
This chapter instructs you on how to connect the Gateway to your network.
- **Chapter 5: Configuring the Wireless-N ADSL2+ Gateway**  
This chapter explains how to configure the Gateway's settings using its Web-based Utility.
- **Appendix A: Troubleshooting**  
This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-N ADSL2+ Gateway.
- **Appendix B: Wireless Security**  
This appendix explains the risks of wireless networking and some solutions to reduce the risks.
- **Appendix C: Finding the MAC Address and IP Address for your Ethernet Adapter.**  
This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Gateway.
- **Appendix D: Upgrading Firmware**  
This appendix instructs you on how to upgrade the firmware on the Gateway if you should need to do so.
- **Appendix E: Glossary**  
This appendix gives a brief glossary of terms frequently used in networking.
- **Appendix F: Specifications**  
This appendix provides the technical specifications for the Gateway.
- **Appendix G: Warranty Information**  
This appendix supplies the warranty information for the Gateway.



## Wireless-N ADSL2+ Gateway

- **Appendix H: Regulatory Information**  
This appendix supplies the regulatory information regarding the Gateway.
- **Appendix I: Contact Information**  
This appendix provides contact information for a variety of Linksys resources, including Technical Support.

# Chapter 2: Planning Your Network

## The Gateway's Functions

A Gateway is a network device that connects two networks together.

In this instance, the Gateway connects your Local Area Network (LAN), or the group of computers in your home or office, to the Internet. The Gateway processes and regulates the data that travels between these two networks.

The Gateway's NAT feature protects your network of computers so users on the public, Internet side cannot "see" your computers. This is how your network remains private. The Gateway protects your network by inspecting every packet coming in through the Internet port before delivery to the appropriate computer on your network. The Gateway inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate computer on the LAN side.

Remember that the Gateway's ports connect to two sides. The LAN ports connect to the LAN, and the ADSL port connects to the Internet. The LAN ports transmit data at 10/100Mbps.

## IP Addresses

### What's an IP Address?

IP stands for Internet Protocol. Every device on an IP-based network, including computers, print servers, and Gateways, requires an IP address to identify its "location," or address, on the network. This applies to both the Internet and LAN connections. There are two ways of assigning an IP address to your network devices. You can assign static IP addresses or use the Gateway to assign IP addresses dynamically.

### Static IP Addresses

A static IP address is a fixed IP address that you assign manually to a computer or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses must be unique and are commonly used with network devices such as server computers or print servers.



Figure 2-1: Network

*ip (internet protocol): a protocol used to send data over a network*



**NOTE:** Since the Gateway is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this User Guide, you'll see references to the "Internet IP address" and the "LAN IP address."

Since the Gateway uses NAT technology, the only IP address that can be seen from the Internet for your network is the Gateway's Internet IP address. However, even this Internet IP address can be blocked, so that the Gateway and network seem invisible to the Internet—see the Security - Firewall tab in "Chapter 5: Configuring the Wireless-N ADSL2+ Gateway."

## Wireless-N ADSL2+ Gateway

Since you use the Gateway to share your DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the Gateway. You can get that information from your ISP.

### Dynamic IP Addresses

A dynamic IP address is automatically assigned to a device on the network, such as computers and print servers. These IP addresses are called “dynamic” because they are only temporarily assigned to the computer or device. After a certain time period, they expire and may change. If a computer logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will automatically assign it a new dynamic IP address.

### DHCP (Dynamic Host Configuration Protocol) Servers

Computers and other network devices using dynamic IP addressing are assigned a new IP address by a DHCP server. The computer or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

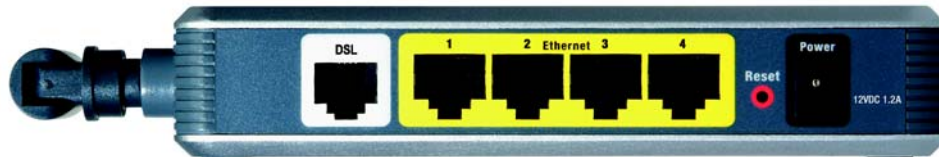
A DHCP server can either be a designated computer on the network or another network device, such as the Gateway. By default, the Gateway’s DHCP Server function is enabled.

If you already have a DHCP server running on your network, you must disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Gateway, see the DHCP section in “Chapter 5: Configuring the Wireless-N ADSL2+ Gateway.”

# Chapter 3: Getting to Know the Wireless-N ADSL2+ Gateway

## Ports and Reset Button on Side Panel

The Gateway's ports and Reset button are located on a side panel.



**Figure 3-1: Ports and Reset Button on Side Panel**

- |                       |                                                                                                                                                                                                                                                                  |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DSL</b>            | The <b>DSL</b> port connects to the ADSL line.                                                                                                                                                                                                                   |
| <b>Ethernet (1-4)</b> | The <b>Ethernet</b> ports connect to your computers and other network devices.                                                                                                                                                                                   |
| <b>Reset Button</b>   | There are two ways to reset the Gateway's factory defaults. Either press the <b>Reset Button</b> , for approximately five seconds, or restore the defaults from the <i>Factory Defaults</i> screen of the Administration tab in the Gateway's Web-based Utility. |
| <b>Power</b>          | The <b>Power</b> port is where you will connect the power adapter.                                                                                                                                                                                               |



**IMPORTANT:** Resetting the Gateway to factory defaults will erase all of your settings (including Internet connection, wireless, and other settings) and replace them with the factory defaults. Do not reset the Gateway if you want to retain these settings.

## LEDs on Side Panel

The Gateway's LEDs, which indicate network activity, are located on the other side panel.



**Figure 3-2: LEDs on Side Panel**

<b>(POWER) button</b>	When you want to power the Gateway on or off, push this button.
<b>POWER</b>	Green. The <b>POWER</b> LED lights up when the Gateway is powered on.
<b>WIRELESS</b>	Green. The <b>WIRELESS</b> LED lights up whenever there is a successful wireless connection. If the LED is flashing, the Gateway is actively sending or receiving data to or from one of the devices on the network.
<b>ETHERNET (1-4)</b>	Green. The <b>ETHERNET</b> LED serves two purposes. If the LED is continuously lit, the Gateway is successfully connected to a device through the Ethernet port. If the LED is flashing, it is an indication of any network activity.
<b>DSL</b>	Green. The <b>DSL</b> LED lights up whenever there is a successful DSL connection. The LED flashes while the Gateway is establishing the ADSL connection.
<b>INTERNET</b>	Green. The <b>INTERNET</b> LED lights up green when an Internet connection to the Internet Service Provider (ISP) is established. The <b>INTERNET</b> LED lights up red when the connection to the ISP fails.

# Chapter 4: Connecting the Wireless-N ADSL2+ Gateway

## Overview

The installation technician from your ISP should have left the setup information with you after installing your broadband connection. If not, you can call your ISP to request that data. After you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Gateway.

To use a computer with an Ethernet adapter to configure the Gateway, continue to “Wired Connection to a Computer.” To use a wireless-equipped computer, continue to “Wireless Connection to a Computer.”

## Wired Connection to a Computer

1. Make sure that all of your network’s hardware is powered off, including the Gateway and all computers.

2. Connect a phone cable from the DSL port on the Gateway’s side panel to the wall jack of the ADSL line. A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.



**NOTE:** A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.

3. Connect one end of an Ethernet network cable to one of the Ethernet ports (labeled 1-4) on the back of the Gateway, and the other end to an Ethernet port on a computer. Repeat this step to connect more computers, a switch, or other network devices to the Gateway.

4. Connect the power adapter to the Gateway’s Power port, and then plug the power adapter into a power outlet.



**NOTE:** You should always plug the Gateway’s power adapter into a power strip with surge protection.

The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, and then it will be solidly lit when the self-test is complete. If the LED flashes for one minute or longer, see “Appendix A: Troubleshooting.”

5. Power on one of your computers that is connected to the Gateway.

**Go to “Chapter 5: Configuring the Wireless-N ADSL2+ Gateway.”**

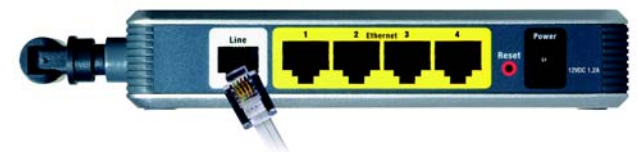


Figure 4-1: Connect the ADSL Line

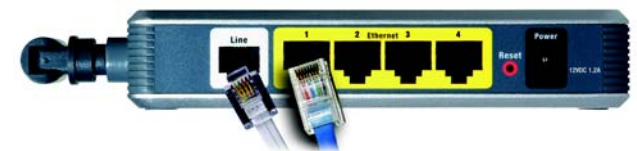


Figure 4-2: Connect a PC

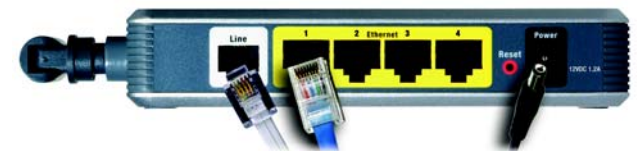


Figure 4-3: Connect the Power

## Wireless Connection to a Computer

If you want to use a wireless connection to access the Gateway, follow these instructions:

1. Make sure that all of your network's hardware is powered off, including the Gateway and all computers.
2. Connect a phone cable from the DSL port on the Gateway's back panel to the wall jack of the ADSL line. A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.



**NOTE:** A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.

3. Connect the power adapter to the Power port, and then plug the power adapter into a power outlet.

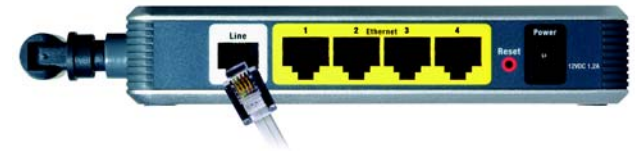


**NOTE:** You should always plug the Gateway's power adapter into a power strip with surge protection.

The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, and then it will be solidly lit when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."

4. Power on one of the computers on your wireless network(s).
5. For initial access to the Gateway through a wireless connection, make sure the computer's wireless adapter has its SSID set to **linksys** (the Gateway's default setting), and its wireless security is disabled. After you have accessed the Gateway, you can change the Gateway and this computer's adapter settings to match your usual network settings.

**Go to "Chapter 5: Configuring the Wireless-N ADSL2+ Gateway."**



**Figure 4-4: Connect the ADSL Line**



**Figure 4-5: Connect the Power**



**NOTE:** You should always change the SSID from its default, **linksys**, and enable wireless security.

# Chapter 5: Configuring the Wireless-N ADSL2+ Gateway

## Overview

Follow the steps in this chapter and use the Gateway's Web-based Utility to configure the Gateway. This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Gateway. For a basic network setup, most users only have to use the following screens of the Utility:

- **Basic Setup.** On the Basic Setup screen, enter the settings provided by your ISP.
- **Management.** Click the **Administration** tab and then the **Management** tab. The Gateway's default username and password is **admin**. To secure the Gateway, change the default username and password.

There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs. Click **Help** for more information.

## Setup

- **Basic Setup.** Enter the Internet connection and network settings on this screen.
- **DDNS.** To enable the Gateway's Dynamic Domain Name System (DDNS) feature, complete the fields on this screen.
- **Advanced Routing.** On this screen, you can alter NAT and routing configurations.

## Wireless

- **Basic Wireless Settings.** You can choose your wireless network settings on this screen.
- **Wireless Security.** Configure your wireless security settings on this screen.
- **Wireless MAC Filter.** This screen lets you control access to your wireless network.
- **Advanced Wireless Settings.** On this screen you can access the advanced wireless network settings.



**HAVE YOU:** Enabled TCP/IP on your computers? Computers communicate over the network with this protocol. Refer to Windows Help for more information on TCP/IP.



**NOTE:** For added security, you should change the username and password through the Administration tab.



## Security

- **Firewall.** Use this screen to enable/disable the firewall, set up filters, and block anonymous Internet requests.
- **VPN Passthrough.** You can enable or disable Virtual Private Network (VPN) Passthrough on this screen.

**vpn** (*virtual private network*): a security measure to protect data as it leaves one network and goes to another over the Internet.

## Access Restrictions

- **Internet Access Policy.** This screen allows you to control the Internet usage and traffic on your local network.

## Applications & Gaming

- **Single Port Range Forwarding.** Use this screen to set up common services or applications that require forwarding on a single port.
- **Port Range Forwarding.** To set up public services or other specialized Internet applications that require forwarding on a range of ports, use this screen.
- **Port Triggering.** To set up triggered ranges and forwarded ranges for Internet applications, click this tab.
- **DMZ.** To allow one local computer to be exposed to the Internet for use of special-purpose services, use this screen.
- **QoS.** Use Quality of Service (QoS) to assign different priority levels to different types of data transmissions.

## Administration

- **Management.** On this screen, alter Gateway access, Simple Network Management Protocol (SNMP), Universal Plug and Play (UPnP), and wireless management settings.
- **Reporting.** If you want to view or save activity logs, click this tab.
- **Diagnostics.** Use this screen to run a Ping test.
- **Backup & Restore.** On this screen, you can back up or restore the Gateway's configuration.
- **Factory Defaults.** If you want to restore the Gateway's factory default settings, use this screen.
- **Firmware Upgrade.** Click this tab if you want to upgrade the Gateway's firmware.

## Status

- Gateway. This screen provides status information about the Gateway.
- Local Network. This provides status information about the local network.
- Wireless. This screen provides status information about the wireless network.
- DSL Connection. This screen provides status information about the DSL connection.

## How to Access the Web-based Utility

To access the Web-based Utility, launch your web browser, and enter the Gateway's default IP address, **192.168.1.1**, in the *Address* field. Then press **Enter**.

A login screen will appear (Windows XP users will see a similar screen). Enter **admin** (the default user name) in the *User Name* field, and enter **admin** (the default password) in the *Password* field. Then click the **OK** button.

## The Setup Tab

### The Basic Setup Tab

The first screen that appears is the Basic Setup tab. This tab allows you to change the Gateway's general settings. Change these settings as described here and click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to cancel your changes. Click **Help** for more information.

### Internet Setup

- Internet Connection Type. The Gateway supports six Encapsulation methods: RFC 1483 Bridged, RFC 1483 Routed, IPoA, RFC 2516 PPPoE, RFC 2364 PPPoA, and Bridge Mode Only. Select the appropriate type of encapsulation from the drop-down menu. Each *Basic Setup* screen and available features will differ depending on what type of encapsulation you select.
- VC Settings. You will configure your Virtual Circuit (VC) settings in this section.
  - Multiplexing: Select **LLC** or **VC**, depending on your ISP.
  - QoS Type: Select from the drop-down menu: **CBR** (Continuous Bit Rate) to specify fixed bandwidth for voice or data traffic; **UBR** (Unspecific Bit Rate) for application that are none-time sensitive, such as e-mail; or **VBR** (Variable Bite Rate) for bursty traffic and bandwidth-sharing with other applications.

Figure 5-1: Basic Setup

## Wireless-N ADSL2+ Gateway

- **Pcr Rate:** For the Peak Cell Rate, divide the DSL line rate by 424 to get the maximum rate the sender can send cells. Enter the rate in the field (if required by your service provider).
  - **Scr Rate:** The Sustain Cell Rate sets the average cell rate that can be transmitted. The SCR value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).
  - **Autodetect:** Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.
  - **Virtual Circuit:** These fields consist of two items: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields.
  - **DSL Modulation:** Select the appropriate mode: **MultiMode**, **T1 .413**, **G.dmt**, **G-lite**, **ADSL2**, or **ADSL2+**. Contact your ISP if you are not sure which mode to use.
- **IP Settings.** Follow the instructions in the section for your type of encapsulation.

## RFC 1483 Bridged

### Dynamic IP

IP Settings. Select **Obtain an IP Address Automatically** if your ISP says you are connecting through a dynamic IP address.

### Static IP

If you are required to use a permanent (static) IP address to connect to the Internet, then select **Use the following IP Address**.

- **Internet IP Address.** This is the Gateway's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- **Subnet Mask.** This is the Gateway's Subnet Mask. Your ISP will provide you with the Subnet Mask.
- **Default Gateway.** Your ISP will provide you with the default Gateway Address, which is the ISP server's IP address.
- **Primary DNS (Required) and Secondary DNS (Optional).** Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

The screenshot shows the configuration interface for an Internet Connection Type set to 'RFC 1483 Bridged'. The interface is split into two main sections: 'VC Settings' and 'IP Settings'.  
**VC Settings:**  
- Encapsulation: RFC 1483 Bridged (dropdown)  
- Multiplexing:  LLC  VC  
- Qos Type: LBR (dropdown)  
- Pcr Rate: [ ] cps  
- Scr Rate: [ ] cps  
- Autodetect:  Enable  Disable  
- Virtual Circuit: VPI (Range 0-255) [ 0 ] VCI (Range 0-65535) [ 35 ]  
- DSL Modulation: MultiMode (dropdown)  
**IP Settings:**  
-  Obtain an IP Address Automatically  
-  Use the following IP Address:  
- Internet IP Address: [ 192 ] [ 168 ] [ 2 ] [ . ] [ 1 ]  
- Subnet Mask: [ 255 ] [ 255 ] [ 255 ] [ . ] [ 0 ]  
- Default Gateway: [ 10 ] [ 0 ] [ 0 ] [ . ] [ 1 ]  
- Primary DNS: [ 10 ] [ 0 ] [ 0 ] [ . ] [ 2 ]  
- Secondary DNS: [ 10 ] [ 0 ] [ 0 ] [ . ] [ 3 ]

Figure 5-2: RFC 1483 Bridged

## RFC 1483 Routed

If you are required to use RFC 1483 Routed, then select **RFC 1483 Routed**.

- Internet IP Address. This is the Gateway's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Gateway's Subnet Mask. Your ISP will provide you with the Subnet Mask.
- Default Gateway. Your ISP will provide you with the default Gateway Address, which is the ISP server's IP address.
- Primary DNS (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

## IPoA

If you are required to use IPoA (IP over ATM), then select **IPoA**.

- Internet IP Address. This is the Gateway's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Gateway's Subnet Mask. Your ISP will provide you with the Subnet Mask.
- Default Gateway. Your ISP will provide you with the default Gateway Address, which is the ISP server's IP address.
- Primary DNS (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

The screenshot shows the configuration interface for the Internet Connection Type. The 'Internet Connection Type' is set to 'RFC 1483 Routed'. Under 'VC Settings', 'Multiplexing' is set to 'VC', 'Gos Type' is 'UBR', and 'Autodetect' is 'Enable'. Under 'IP Settings', the Internet IP Address is 192.168.2.1, Subnet Mask is 255.255.255.0, Default Gateway is 10.0.0.1, Primary DNS is 10.0.0.2, and Secondary DNS is 10.0.0.3.

Section	Field	Value
Internet Connection Type	Encapsulation:	RFC 1483 Routed
	Multiplexing:	VC
	Gos Type:	UBR
	Pcr Rate:	cps
	Scr Rate:	cps
	Autodetect:	Enable
	Virtual Circuit:	0 VPI (Range 0-255)
		35 VCI (Range 0-65535)
	DSL Modulation:	MultiMode
	IP Settings	Internet IP Address:
Subnet Mask:		255.255.255.0
Default Gateway:		10.0.0.1
Primary DNS:		10.0.0.2
Secondary DNS:		10.0.0.3

Figure 5-3: RFC 1483 Routed

The screenshot shows the configuration interface for the Internet Connection Type. The 'Internet Connection Type' is set to 'IPoA'. Under 'VC Settings', 'Multiplexing' is set to 'VC', 'Gos Type' is 'UBR', and 'Autodetect' is 'Enable'. Under 'IP Settings', the Internet IP Address is 192.168.2.1, Subnet Mask is 255.255.255.0, Default Gateway is 10.0.0.1, Primary DNS is 10.0.0.2, and Secondary DNS is 10.0.0.3.

Section	Field	Value
Internet Connection Type	Encapsulation:	IPoA
	Multiplexing:	VC
	Gos Type:	UBR
	Pcr Rate:	cps
	Scr Rate:	cps
	Autodetect:	Enable
	Virtual Circuit:	0 VPI (Range 0-255)
		35 VCI (Range 0-65535)
	DSL Modulation:	MultiMode
	IP Settings	Internet IP Address:
Subnet Mask:		255.255.255.0
Default Gateway:		10.0.0.1
Primary DNS:		10.0.0.2
Secondary DNS:		10.0.0.3

Figure 5-4: IPoA

## RFC 2516 PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE.

- **User Name and Password.** Enter the User Name and Password provided by your ISP.
- **Connect on Demand: Max Idle Time.** You can configure the Gateway to disconnect the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, click the **Connect on Demand** radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Keep Alive: Redial Period.** If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, click the **Keep Alive** radio button. In the *Redial Period* field, specify how often you want the Gateway to check the Internet connection. The default Redial Period is **30** seconds.

## RFC 2364 PPPoA

Some DSL-based ISPs use PPPoA (Point-to-Point Protocol over ATM) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoA. If they do, you will have to enable PPPoA.

- **User Name and Password.** Enter the User Name and Password provided by your ISP.
- **Connect on Demand: Max Idle Time.** You can configure the Gateway to disconnect the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, click the **Connect on Demand** radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.

**Keep Alive: Redial Period.** If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, click the **Keep Alive** radio button. In the *Redial Period* field, specify how often you want the Gateway to check the Internet connection. The default Redial Period is **30** seconds.

The screenshot shows the configuration interface for RFC 2516 PPPoE. It is divided into two main sections: 'VC Settings' and 'PPPoE Settings'. In the 'VC Settings' section, 'Encapsulation' is set to 'RFC 2516 PPPoE', 'Multiplexing' is set to 'VC' (radio button selected), 'Qos Type' is 'UBR', and 'Autodetect' is set to 'Enable'. In the 'PPPoE Settings' section, 'Username' is 'user123@abcisp.net', 'Password' is masked with asterisks, and the 'Connect on Demand: Max Idle Time' is set to 5 minutes.

Figure 5-5: RFC 2516 PPPoE



**IMPORTANT:** For Connect on Demand to work correctly, close all Internet applications or the Gateway may not drop the connection depending on how often the application tries to get on the Internet (e.g., chat programs).

The screenshot shows the configuration interface for RFC 2364 PPPoA. It is divided into two main sections: 'VC Settings' and 'PPPoA Settings'. In the 'VC Settings' section, 'Encapsulation' is set to 'RFC 2364 PPPoA', 'Multiplexing' is set to 'VC' (radio button selected), 'Qos Type' is 'UBR', and 'Autodetect' is set to 'Enable'. In the 'PPPoA Settings' section, 'Username' is 'user123@abcisp.net', 'Password' is masked with asterisks, and the 'Connect on Demand: Max Idle Time' is set to 5 minutes.

Figure 5-6: RFC 2364 PPPoA

## Bridge Mode Only

If you are using your Gateway as a bridge, which makes the Gateway act like a stand-alone modem, select **Bridge Mode Only**. All NAT and routing settings are disabled in this mode.

## Optional Settings (required by some ISPs)

- **Host Name and Domain Name.** These fields allow you to supply a host and domain name for the Gateway. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, you can leave these fields blank.
- **MTU and Size.** The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select **Manual** and enter the value desired in the *Size* field. It is recommended that you leave this value in the 1200 to 1500 range. By default, MTU is configured automatically.

## Network Setup

- **Router IP.** The values for the Gateway's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work.
  - **Local IP Address.** The default value is **192.168.1.1**.
  - **Subnet Mask.** The default value is **255.255.255.0**.
- **Network Address Server Settings (DHCP).** Configure the Gateway's Dynamic Host Configuration Protocol (DHCP) settings in this section.
  - **DHCP Server.** A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each computer on your network for you. Unless you already have one, it is highly recommended that you leave the Gateway enabled as a DHCP server. You can also use the Gateway in DHCP Relay mode. (This setting is not available for all Encapsulation types.)
  - **DHCP Server.** If you enable the DHCP Relay mode for the *DHCP Server* setting, enter the IP address for the DHCP relay server in the fields provided. (This setting is not available for all Encapsulation types.)
  - **Starting IP Address.** Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1.2 or greater, because the default IP address for the Gateway is **192.168.1.1**.
  - **Maximum Number of DHCP Users.** Enter the maximum number of users/clients that can obtain an IP address. The number will vary depending on the starting IP address entered.

The screenshot shows the 'Internet Connection Type' configuration page. The 'VC Settings' section is active, and 'Bridge Mode Only' is selected in the 'Encapsulation' dropdown. Other settings include: Multiplexing (LLC selected, VC unselected), Qos Type (UBR selected), Pcr Rate (empty), Scr Rate (empty), Autofdetect (Enable selected, Disable unselected), Virtual Circuit (0 selected), VPI (Range 0-255) (empty), VCI (Range 0-65535) (35 selected), and DSL Modulation (MultiMode selected).

Figure 5-7: Bridge Mode Only

The screenshot shows the 'Optional Settings (required by some ISPs)' page. The 'Network Setup' section includes: Host Name (empty), Domain Name (empty), MTU (Auto selected), and Size (1500). The 'Network Address Server Settings (DHCP)' section includes: Local IP Address (192.168.1.1), Subnet Mask (255.255.255.0), DHCP Server (Enable selected, Disable unselected, DHCP Relay unselected), DHCP Server (empty), Starting IP Address (192.168.1.100), Maximum Number of DHCP Users (50), Client Lease Time (0 minutes), Static DNS 1, 2, and 3 (all empty), and WINS (empty). The 'Time Settings' section includes: Time Zone (GMT-08:00 Pacific Time (USA & Canada) selected) and a checkbox for 'Automatically adjust clock for daylight saving changes' (unchecked).

Figure 5-8: Optional Settings

## Wireless-N ADSL2+ Gateway

- **Client Lease Time.** The Client Lease Time is the amount of time a computer will be allowed connection to the Gateway with its current dynamic IP address. Enter the amount of time, in minutes, that the computer will be “leased” this dynamic IP address.
- **Static DNS 1-3.** The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. You can enter up to three DNS Server IP Addresses here. The Gateway will use these for quicker access to functioning DNS servers.
- **WINS.** The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server’s IP address here. Otherwise, leave this field blank.
- **Time Setting.** Select the appropriate time zone for the Gateway’s location. If desired, check the **Automatically adjust clock for daylight saving changes** checkbox.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.

## The DDNS Tab

The Gateway offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Gateway.

Before you can use this feature, you need to sign up for DDNS service at DynDNS.org or TZO.com.

### DDNS

DDNS Service. If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** from the drop-down menu. If your DDNS service is provided by TZO.com, then select **TZO.com** from the drop-down menu. To disable DDNS Service, select **Disabled**.

#### DynDNS.org

- User Name, Password, and Host Name. Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.
- Status. The status of the DDNS service connection is displayed here.
- Connect. Click the **Connect** button to start the DDNS service connection.

#### TZO.com

- E-mail Address, Password, and Domain Name. Enter the E-mail Address, Password, and Domain Name of the account you set up with TZO.
- Status. The status of the DDNS service connection is displayed here.
- Connect. Click the **Connect** button to start the DDNS service connection.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-9: DDNS - DynDNS.org



Figure 5-10: DDNS - TZO.com



## The Advanced Routing Tab

The *Advanced Routing* screen allows you to configure the NAT, dynamic routing, and static routing settings.

### Advanced Routing

- **Operating Mode.** In this section, you will configure the Gateway's general routing settings.
  - **NAT.** NAT is a security feature that is enabled by default. It enables the Gateway to translate IP addresses of your local area network to a different IP address for the Internet. To disable NAT, click the **Disabled** radio button.
- **Dynamic Routing.** With Dynamic Routing you can enable the Gateway to automatically adjust to physical changes in the network's layout. Using RIP, the Gateway determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other Gateways on the network.
  - **RIP.** If you have multiple routers, you may want to use the Routing Information Protocol (RIP) so the routers can exchange routing information with each other. To use RIP, select the **Enabled** radio button. Otherwise, keep the default, **Disabled**.
  - **RIP Version.** Select the protocol version you want, **RIP1** or **RIPv2**.
- **Static Routing.** If the Gateway is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To create a static route, change the following settings:
  - **Select set number.** Select the number of the static route from the drop-down menu. The Gateway supports up to 20 static route entries. If you need to delete a route, then select the entry and click the **Delete This Entry** button.
  - **Destination IP Address.** The Destination IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0.
  - **Subnet Mask.** Enter the Subnet Mask (also known as the Network Mask), which determines which portion of an IP address is the network portion, and which portion is the host portion.
  - **Gateway.** Enter the IP address of the gateway device that allows for contact between the Gateway and the remote network or host.

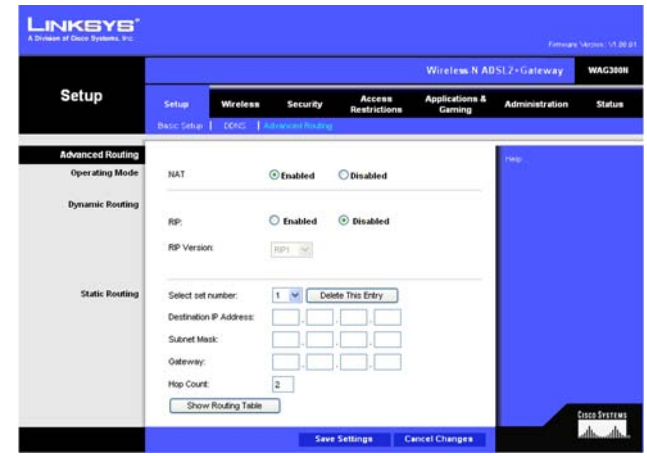


Figure 5-11: Advanced Routing

## Wireless-N ADSL2+ Gateway

- **Hop Count.** Hop Count is the number of hops to each node until the destination is reached (16 hops maximum). Enter the Hop Count in the field provided.
- **Show Routing Table.** Click the **Show Routing Table** button to open a screen displaying how data is routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click the **Refresh** button to update the information. Click the **Close** button to return to the previous screen.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



The screenshot shows the Linksys web interface with the 'Routing Table' tab selected. The page title is 'LINKSYS A Division of Cisco Systems, Inc.'. Below the title, there is a 'Routing Table' tab and a 'Routing Table Entry List' section. The 'Routing Table Entry List' contains a table with the following data:

Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	192.168.1.1	LAN
192.168.1.0	255.255.255.0	0.0.0.0	LAN
192.168.1.0	255.255.255.0	192.168.1.1	LAN
239.0.0.0	255.0.0.0	0.0.0.0	LAN

There is a 'Refresh' button above the table and a 'Close' button below it.

**Figure 5-12: Routing Table**

## The Wireless Tab

### The Basic Wireless Settings Tab

This screen allows you to choose your wireless network mode and wireless security.

#### Wireless Network

- **Network Mode.** If you have 802.11g and 802.11b devices in your network, then keep the default setting, **Mixed**. If you have only Wireless-G devices, select **Wireless-G Only**. If you have only Wireless-B devices, select **Wireless-B Only**. If you have only Wireless-N devices, select **Wireless-N Only**. If you want to disable wireless networking, select **Disable**.
- **Network Name (SSID).** Enter the name for your wireless network into the field. The SSID is the network name shared among all devices in a wireless network. It must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Linksys recommends that you change the default SSID (linksys) to a unique name of your choice.
- **Radio Band.** For best performance in a network using Wireless-N, Wireless-G and Wireless-B devices, keep the default, **Wide - 40MHz Channel**. For Wireless-G and Wireless-B networking only, select **Standard - 20MHz Channel**.
- **Wide Channel.** If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu.
- **Standard Channel.** Select the channel for Wireless-N, Wireless-G, and Wireless-B networking. If you selected Wide – 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N. If you are not sure which channel to select, do not make any changes.
- **Wireless SSID Broadcast.** When wireless computers or clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Gateway. To broadcast the Gateway's SSID, keep the default setting, **Enable**. If you do not want to broadcast the Gateway's SSID, then select **Disable**.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-13: Basic Wireless Settings



**NOTE:** If you select Wide - 40MHz Channel for the Radio Band setting, then Wireless-N can use two channels: a primary one (Wide Channel) and a secondary one (Standard Channel). This will enhance Wireless-N performance.

## The Wireless Security Tab

The Wireless Security settings configure the security of your wireless network. There are six wireless security options supported by the Gateway: PSK-Personal, PSK2-Personal, PSK-Enterprise, PSK2-Enterprise, RADIUS, and WEP. PSK stands for Pre-Shared Key, which is a security standard stronger than WEP (Wired Equivalent Privacy) encryption. PSK2 is a more advanced, more secure version of PSK. PSK-Enterprise, PSK2-Enterprise, and RADIUS use a RADIUS (Remote Authentication Dial-In User Service) server for authentication. These are briefly discussed here. For detailed instructions on configuring wireless security for the Gateway, turn to “Appendix B: Wireless Security.”

If you want to disable wireless security, select **Disable** from the drop-down menu for Security Mode.

- Security Mode. Select the mode you want your network to use, **PSK-Personal**, **PSK2-Personal**, **PSK-Enterprise**, **PSK2-Enterprise**, **RADIUS**, or **WEP**. If you have devices using PSK-Personal and PSK2-Personal, select **PSK2-Personal**.

### PSK-Personal

- Encryption. Select the method you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)
- Pre-shared Key. Enter the key shared by the Gateway and your other network devices. It must have 8 to 63 characters.
- Key Renewal. Enter the Key Renewal period, which tells the Gateway how often it should change the dynamic encryption keys.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.

### PSK2-Personal

- Encryption. Select the method you want to use, **AES** or **TKIP** or **AES**.
- Pre-shared Key. Enter the key shared by the Gateway and your other network devices. It must have 8 to 63 characters.
- Key Renewal. Enter the Key Renewal period, which tells the Gateway how often it should change the dynamic encryption keys.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-14: Wireless Security - PSK-Personal



**IMPORTANT:** If you are using wireless security, always remember that each device in your wireless network **MUST** use the same wireless security method and shared key, or else the network will not function correctly. If you have devices using PSK-Personal and PSK2-Personal, you should use PSK2-Personal.



Figure 5-15: Wireless Security - PSK2-Personal

## PSK-Enterprise

PSK-Enterprise features PSK used with a RADIUS server. (This method should only be used when the Gateway is connected to a RADIUS server.)

- Encryption. Select the method you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)
- RADIUS Server. Enter the IP address of the RADIUS server.
- RADIUS Port. Enter the port number of the RADIUS server.
- Shared Key. Enter the key shared between the Gateway and its RADIUS server.
- Key Renewal. Enter the Key Renewal period, which tells the Gateway how often it should change the dynamic encryption keys.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.

## PSK2-Enterprise

PSK2-Enterprise features PSK2 used with a RADIUS server. (This method should only be used when the Gateway is connected to a RADIUS server.)

- Encryption. Select the method you want to use, **AES** or **TKIP** or **AES**.
- RADIUS Server. Enter the IP address of the RADIUS server.
- RADIUS Port. Enter the port number of the RADIUS server.
- Shared Key. Enter the key shared between the Gateway and its RADIUS server.
- Key Renewal. Enter the Key Renewal period, which tells the Gateway how often it should change the dynamic encryption keys.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-16: Wireless Security - PSK-Enterprise



Figure 5-17: Wireless Security - PSK2-Enterprise

## RADIUS

This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Gateway.)

- **RADIUS Server.** Enter the IP address of the RADIUS server.
- **RADIUS Port.** Enter the port number of the RADIUS server.
- **Shared Key.** Enter the key shared between the Gateway and its RADIUS server.
- **Encryption.** Select the appropriate level of encryption, **40/64-bit (10 hex digits)** or **104/128-bit (26 hex digits)**. A higher level of encryption is more secure.
- **Passphrase.** Instead of manually entering WEP keys, you can enter a Passphrase. It is case-sensitive and should not be longer than 32 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only and cannot be used with Windows XP Zero Configuration. If you want to communicate with non-Linksys wireless products or Windows XP Zero Configuration, make a note of the WEP keys generated, and enter the appropriate one manually in the wireless computer or client.) If you want to use a Passphrase, then enter it in the *Passphrase* field and click the **Generate** button.
- **Keys 1-4.** If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes; they are not valid key values.) If you are using 40/64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 104/128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0”-“9” and “A”-“F”.
- **TX Key.** To indicate which WEP key to use, select a default Transmit (TX) Key number.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.



Figure 5-18: Wireless Security - RADIUS

## WEP

- **Encryption.** Select the appropriate level of encryption, **40/64-bit (10 hex digits)** or **104/128-bit (26 hex digits)**. A higher level of encryption is more secure.
- **Passphrase.** Instead of manually entering WEP keys, you can enter a Passphrase. It is case-sensitive and should not be longer than 32 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only and cannot be used with Windows XP Zero Configuration. If you want to communicate with non-Linksys wireless products or Windows XP Zero Configuration, make a note of the WEP keys generated, and enter the appropriate one manually in the wireless computer or client.) If you want to use a Passphrase, then enter it in the *Passphrase* field and click the **Generate** button.
- **Keys 1-4.** If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes; they are not valid key values.) If you are using 40/64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 104/128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0”-“9” and “A”-“F”.
- **TX Key.** To indicate which WEP key to use, select a default Transmit (TX) Key number.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



**Figure 5-19: Wireless Security - WEP**

## The Wireless MAC Filter Tab

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.

### Wireless MAC Filter

To filter wireless users by MAC Address, either permitting or blocking access, click **Enabled**. If you do not wish to filter users by MAC Address, select **Disabled**.

#### Access Restrictions

- **Prevent.** Click this button to block wireless access from the devices listed on this screen.
- **Permit.** Click this button to allow wireless access by the devices listed on this screen.

#### MAC Address Filter List

Click the **Wireless Client List** button to display the Wireless Client List. It shows computers and other devices on the wireless network. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Status. Click the **Save to MAC Address Filter List** checkbox for any device you want to add to the MAC Address Filter List. Then click the **Add** button. To retrieve the most up-to-date information, click the **Refresh** button. To exit this screen and return to the *Wireless MAC Filter* screen, click the **Close** button.

**MAC 01-50.** Enter the MAC addresses of the devices whose wireless access you want to block or allow.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.

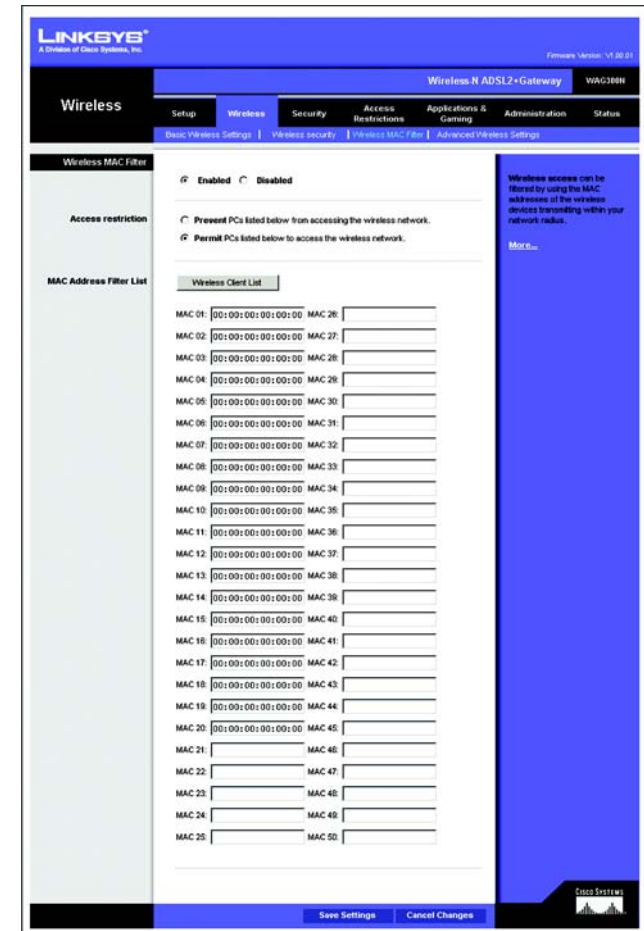


Figure 5-20: Wireless MAC Filter



Figure 5-21: Wireless Client List



## The Advanced Wireless Settings Tab

This tab is used to set up the Gateway's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

### Advanced Wireless

- **AP Isolation.** This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Gateway but not with each other. To use this function, click **Enabled**. AP Isolation is disabled by default.
- **Authentication Type.** The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. Select **Shared Key** if you only want to use Shared Key authentication (the sender and recipient use a WEP key for authentication).
- **Basic Rate.** The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Gateway can transmit. The Gateway will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Gateway will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Gateway can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Gateway can transmit at all wireless rates.
- **Transmission Rate.** The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Gateway and a wireless client. The default setting is **Auto**.
- **N Transmission Rate.** The rate of data transmission should be set depending on the speed of your Wireless-N networking. You can select from a range of transmission speeds, or you can select **Auto** to have the Gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Gateway and a wireless client. The default setting is **Auto**.
- **CTS Protection Mode.** CTS (Clear-To-Send) Protection Mode's default setting is **Auto**. The Gateway will automatically use CTS Protection Mode when your Wireless-N and Wireless-G products are experiencing severe problems and are not able to transmit to the Gateway in an environment with heavy 802.11b traffic. This function boosts the Gateway's ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance.

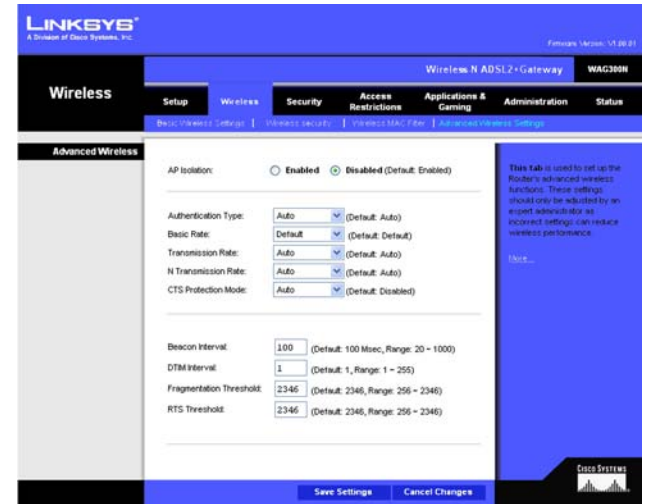


Figure 5-22: Advanced Wireless Settings

## Wireless-N ADSL2+ Gateway

- **Beacon Interval.** Enter a value between 20-1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Gateway to synchronize the wireless network. The default value is **100**.
- **DTIM Interval.** This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Gateway has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.
- **Fragmentation Threshold.** This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.
- **RTS Threshold.** Should you encounter inconsistent data flow, only minor reduction of the default value, **2346**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Gateway sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. In most cases, keep its default value of **2346**.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.

## The Security Tab

### The Firewall Tab

You can enable or disable the firewall, select filters to block specific Internet data types, and block anonymous Internet requests. Use these features to enhance the security of your network.

#### Firewall

- **SPI Firewall Protection.** The Stateful Packet Inspection (SPI) firewall feature enhances the security of your network. To use this feature, click **Enable**. If you do not want to use the firewall, click **Disable**.

#### Additional Filters

- **Filter Proxy.** Use of WAN proxy servers may compromise the Gateway's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click the checkbox.
- **Filter Cookies.** A cookie is data stored on your computer and used by Internet sites when you interact with them. To enable cookie filtering, click the checkbox.
- **Filter Java Applets.** Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using this programming language. To enable Java Applet filtering, click the checkbox.
- **Filter ActiveX.** ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click the checkbox.

#### Block WAN Requests

- **Block Anonymous Internet Requests.** This keeps your network from being “pinged” or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to discover your network. Select **Block Anonymous Internet Requests** to block anonymous Internet requests or de-select it to allow anonymous Internet requests.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-23: Firewall

## The VPN Passthrough Tab

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. Configure these settings so the Gateway will permit VPN tunnels to pass through.

### VPN Passthrough

- **IPSec Passthrough.** Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enable** button. To disable IPSec Passthrough, click the **Disable** button.
- **PPTP Passthrough.** Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP Passthrough, click the **Enable** button. To disable PPTP Passthrough, click the **Disable** button.
- **L2TP Passthrough.** Layering 2 Tunneling Protocol Passthrough is an extension of the Point-to-Point Tunneling Protocol (PPTP) used to enable the operation of a VPN over the Internet. To allow L2TP Passthrough, click the **Enable** button. To disable L2TP Passthrough, click the **Disable** button.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-24: VPN Passthrough

## The Access Restrictions Tab

### The Internet Access Policy Tab

The *Internet Access Policy* screen allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific computers and block websites by URL address or keyword.

#### Internet Access Policy

Internet Access Policy. Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the **Delete** button. To view all the policies, click the **Summary** button. (Policies can be deleted from the *Summary* screen by selecting the policy or policies and clicking the **Delete** button. To return to the Internet Access screen, click the **Close** button.)

Status. Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and click the radio button beside *Enable*.

To create an Internet Access policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, click the radio button beside *Enable*.
3. Enter a Policy Name in the field provided.

Figure 5-25: Internet Access Policy

No.	Policy Name	Days (Sun - Sat)	Time of Day	Delete
1.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>
2.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>
3.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>
4.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>
5.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>
6.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>
7.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>
8.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>
9.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>
10.		S M T W T F S	00:00 - 00:00	<input type="checkbox"/>

Figure 5-26: Internet Policy Summary

4. Click the **Edit List of PCs** button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button to exit this screen.
5. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
7. If you want to block websites with specific URL addresses, enter each URL in a separate field next to *Website Blocking by URL Address*.
8. If you want to block websites using specific keywords, enter each keyword in a separate field next to *Website Blocking by Keyword*.
9. You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*. The port numbers and protocol for the selected service will be automatically displayed.  
  
If the service you want is not listed, select **User-Defined**. Enter its port numbers in the fields provided. Then select its protocol, **ICMP**, **TCP**, **UDP**, or **TCP & UDP** from the drop-down menu.
10. Click the **Save Settings** button to save the policy's settings. To undo the policy's settings, click the **Cancel Changes** button. Click **Help** for more information.

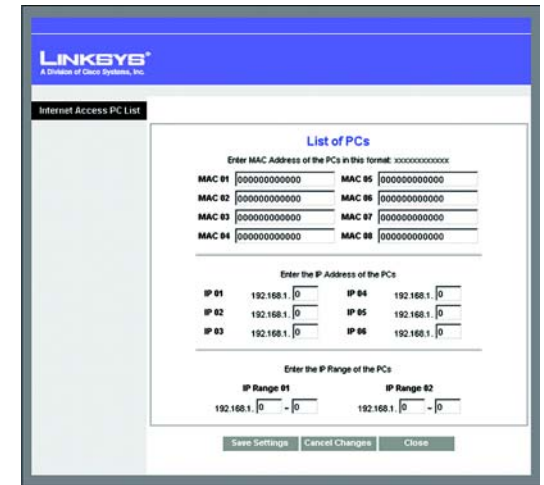


Figure 5-27: List of PCs

## The Applications and Gaming Tab

### The Single Port Range Forwarding Tab

Use the *Single Port Range Forwarding* screen when you want to open a specific port so users on the Internet can see the servers behind the Gateway (such servers may include FTP or e-mail servers). When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

#### Single Port Forwarding

- Application. Enter the name of the application in the field provided.
- External Port and Internal Port. Enter the External and Internal Port numbers.
- Protocol. Select the protocol you wish to use for each application: **TCP** or **UDP**.
- IP Address. Enter the IP Address of the appropriate computer.
- Enabled. Click **Enabled** to enable forwarding for the chosen application.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-28: Single Port Forwarding

## The Port Range Forwarding Tab

The *Port Range Forwarding* screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

### Port Range Forwarding

- **Application.** Enter the name of the application in the field provided.
- **Start and End.** Enter the starting and ending numbers of the port range you wish to forward.
- **Protocol.** Select the protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- **IP Address.** Enter the IP Address of the appropriate computer.
- **Enable.** Click the **Enable** checkbox to enable forwarding for the chosen application.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.

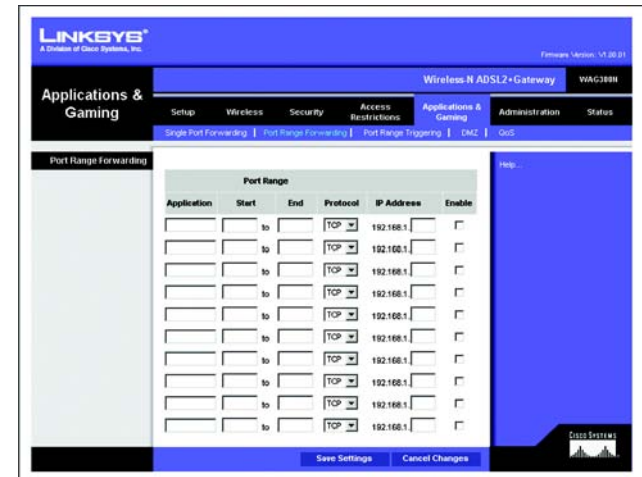


Figure 5-29: Port Range Forwarding



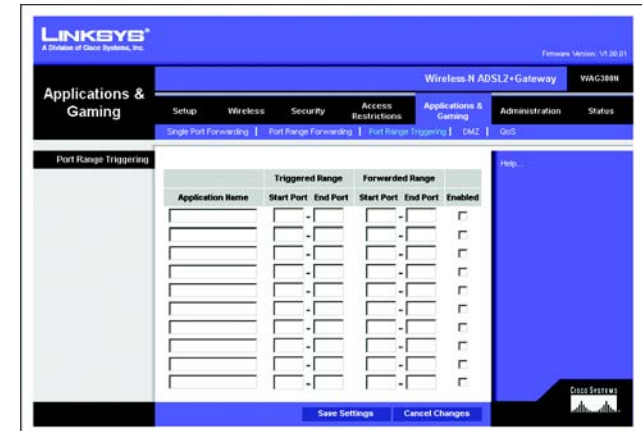
## The Port Triggering Tab

Port Triggering is used for special applications that can request a port to be opened on demand. For this feature, the Gateway will watch outgoing data for specific port numbers. The Gateway will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Gateway, the data is pulled back to the proper computer by way of IP address and port mapping rules.

### Port Range Triggering

- Application. Enter the name you wish to give each application.
- Triggered Range. Enter the starting and ending port numbers of the Triggered Range.
- Forwarded Range. Enter the starting and ending port numbers of the Forwarded Range.
- Enabled. Click the **Enabled** checkbox to enable port triggering for the chosen application.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



**Figure 5-30: Port Triggering**

## The DMZ Tab

The *DMZ* screen allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing through DMZ Hosting. DMZ hosting forwards all the ports for one computer at the same time, which differs from Port Range Forwarding, which can only forward a maximum of 10 ranges of ports.

### DMZ

- **DMZ Hosting.** This feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enable**. To disable DMZ, select **Disable**.
- **DMZ Host IP Address.** To expose one computer, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-31: DMZ

## The QoS Tab

### QoS (Quality of Service)

QoS ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as Internet phone calls or videoconferencing.

#### Wireless

- **ACK Mode.** This setting prioritizes QoS for users who also have ACK Mode enabled. Users with Immediate ACK (the default setting) will experience reliable connectivity for normal network use. Burst ACK is faster but less reliable and may also affect long-range wireless performance. The No ACK setting disables the ACK feature. Clients utilizing ACK must have their wireless adapter on the same setting as the Gateway. This is normally used in a multicast broadcast like video. Do not use this unless you are an advanced user.
- **802.11e/QoS.** QoS will be enabled by default to provide the best performance for your wireless connection. Select **Disable** to improve performance for a mixed wireless network.

#### Internet Access Priority

In this section, you can set priority based on Application, Port Range, or MAC Address. There are four priorities you can set: High, Medium, Normal, or Low.

- **Enabled/Disabled.** To limit outgoing bandwidth for the QoS policies in use, select **Enabled**. Otherwise, select **Disabled**.
- **Set Internet Bandwidth.** This setting allows you to limit the outgoing bandwidth for the QoS policies in use, so you can control how much bandwidth a particular application is allowed to use. Enter the bandwidth in the field.
- **Application.** With this option you can select **None**, **Online Game**, **MSN Messenger**, **YAHOO Messenger**, **Skype**, **Voice Device**, **Add a New Application**, or select from the list of applications you want to set. To create a new entry, select **Add a New Application**, and refer to the *Add a New Application* section.
- **Priority.** Select **High**, **Medium**, **Normal**, or **Low** for the bandwidth priority you need for the application you selected. Don't set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select **Low**. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority. Once you have made your selection, click **Add** to add to the Summary list.



Figure 5-32: QoS

## Wireless-N ADSL2+ Gateway

### Online Game

**Select a Game** Select a game from the drop-down menu, which lists some common pre-configured games.

**Priority** Select its priority from the drop-down menu, and click **Add**.

### MSN Messenger

Select its priority from the drop-down menu, and click **Add**.

### YAHOO Messenger

Select its priority from the drop-down menu, and click **Add**.

### Skype

Select its priority from the drop-down menu, and click **Add**.

### Voice Device

**Enter a Name** Enter the name of your network device.

**MAC Address** Enter its MAC Address.

**Priority** Select its priority from the drop-down menu, and click **Add**.

### Add a New Application

**Enter a Name** Enter any name to indicate the name of the entry.

**Category** Select from **Port Range** or **MAC Address** for the Gateway to use to set the bandwidth priority.

**Port Range** If you selected Port Range, then this category will be available. It allows you to enter the port range(s) that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

You can define up to three ranges for this bandwidth allocation. For each port range, designate the protocol type(s): **TCP**, **UDP**, or **Both**.

**MAC Address** If you selected MAC Address, then this category will be available. Enter the 12 hexadecimal digit MAC Address to represent the device you want to set as a bandwidth priority. This is a



Figure 5-33: QoS - Online Game



Figure 5-34: QoS - MSN Messenger

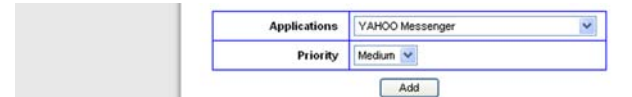


Figure 5-35: QoS - YAHOO Messenger



Figure 5-36: QoS - Skype

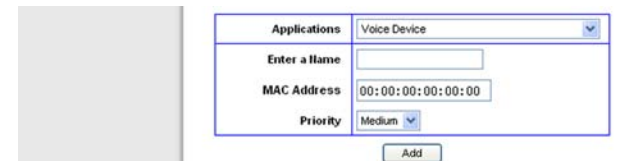


Figure 5-37: QoS - Voice Device



Figure 5-38: QoS - Add a New Application (Port Range)

## Wireless-N ADSL2+ Gateway

unique identifier for your network device. When the Gateway identifies the device entered, the Gateway will allocate the priority set for that entry. Check the device's documentation to obtain the MAC Address.

**Priority** Select the bandwidth priority for the application you selected. Select **High**, **Medium**, **Normal**, or **Low** for the bandwidth, but don't set all applications to High. Once you have made your selection, click **Add** to add to the Summary list.

### Summary

**Priority** This displays the bandwidth allocation priority of High, Medium, Normal, or Low, that you set for the application.

**Name** This displays the application name or the entries you entered to be allocated.

**Information** This displays the Port Range or MAC Address entered when you added a new application. If a pre-configured application was selected, there will be no valid entry shown in this section.

**Remove** This button allows you to remove the application entry. To remove the entry, click the **Remove** button. To save the configuration, click the **Save Settings** button. Otherwise, to cancel, click the **Cancel Changes** button.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



The screenshot shows a web-based configuration form titled "Add a New Application". The form has a title bar "Applications" with a dropdown menu showing "Add a New Application". Below the title bar, there are four input fields: "Enter a Name" (a text box), "Category" (a dropdown menu with "MAC Address" selected), "MAC Address" (a text box containing "00:00:00:00:00:00"), and "Priority" (a dropdown menu with "Medium" selected). At the bottom right of the form is an "Add" button.

**Figure 5-39: QoS - Add a New Application (MAC Address)**

## The Administration Tab

### The Management Tab

The *Management* screen allows you to change the Gateway's access settings as well as configure the SNMP (Simple Network Management Protocol), UPnP (Universal Plug and Play), and WLAN management features.

### Gateway Access

**Local Gateway Access.** To ensure the Gateway's security, you will be asked for your password when you access the Gateway's Web-based Utility. The default username and password is **admin**.

- **Gateway Userlist.** Select the number of the user from the drop-down menu.
- **Gateway Username.** Enter the default username, **admin**. It is recommended that you change the default username to one of your choice.
- **Gateway Password.** It is recommended that you change the default password, **admin**, to one of your choice.
- **Re-enter to confirm.** Re-enter the Gateway's new Password to confirm it.

**Remote Gateway Access.** This feature allows you to access the Gateway from a remote location, via the Internet.

- **Remote Management.** This feature allows you to manage the Gateway from a remote location via the Internet. To enable Remote Management, click **Enable**.



**IMPORTANT:** Enabling remote management allows anyone with your password to configure the Gateway from somewhere else on the Internet.

- **Management Port.** Enter the port number you will use to remotely access the Gateway.

### SNMP

SNMP is a popular network monitoring and management protocol.

- **Device Name.** Enter the name of the Gateway.
- **SNMP.** To enable SNMP, click **Enable**. To disable SNMP, click **Disable**.
- **Get Community.** Enter the password that allows read-only access to the Gateway's SNMP information.

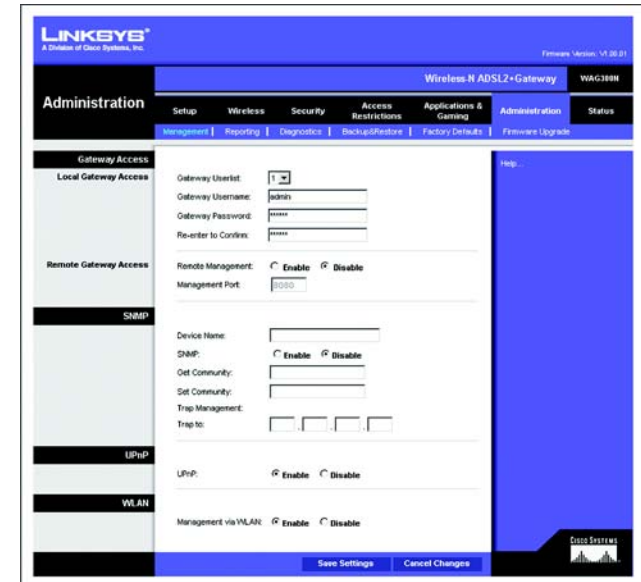


Figure 5-40: Management

## Wireless-N ADSL2+ Gateway

- **Set Community.** Enter the password that allows read/write access to the Gateway's SNMP information.
- **Trap Management: Trap to.** Enter the IP address of the remote host computer that will receive the trap messages.

## UPnP

UPnP allows Windows Me and XP to automatically configure the Gateway for various Internet applications, such as gaming and videoconferencing.

- **UPnP.** To enable UPnP, click **Enable**. Otherwise, click **Disable**.

## WLAN

- **Management via WLAN.** This feature allows the Gateway to be managed by a wireless computer on the local network when it logs into the Gateway's Web-based Utility. To enable this feature, click **Enable**. Otherwise, click **Disable**.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.

## The Reporting Tab

The *Reporting* screen provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection. It also provides logs for VPN and firewall events.

### Reporting

- Log. To enable log reporting, click **Enable**.

### Email Alerts

- E-Mail Alerts. To enable E-Mail Alerts, click **Enable**.
- Denial of Service Thresholds. Enter the number of Denial of Service attacks that will trigger an e-mail alert.
- SMTP Mail Server. Enter the IP address of the SMTP server.
- E-Mail Address for Alert Logs. Enter the e-mail address that will receive alert logs.
- Return E-Mail address. Enter the return address for the e-mail alerts.

To view the logs, click the **View Logs** button. A new screen will appear. From the drop-down menu, select which log you want to view: **ALL**, **System Log**, **Access Log**, or **Firewall Log**. Click the **pageRefresh** button to refresh the information. Click the **Clear** button to clear the log information. Click the **Previous Page** button to go to the previous page of information. Click the **Next Page** button to move to the next page of information.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-41: Reporting

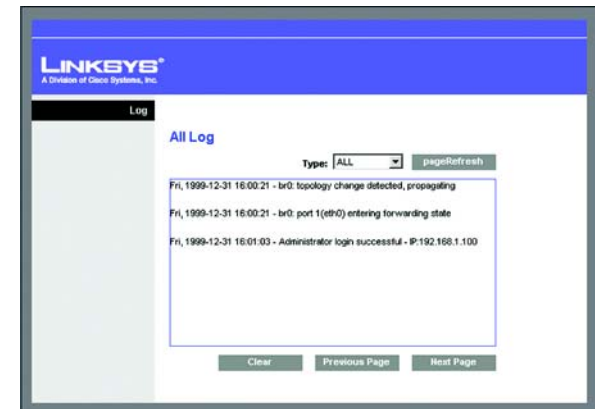


Figure 5-42: View Log



## The Diagnostics Tab

Use this screen to run ping tests and display test results.

### Ping Test

#### Ping Test Parameters

- Ping Target IP. Enter the IP address that you want to ping. This can be either a local (LAN) IP or an Internet (WAN) IP address.
- Ping Size. Enter the size of the packet.
- Number of Pings. Enter the number of times that you want to ping.
- Ping Interval. Enter the ping interval (how often the target IP address will be pinged) in milliseconds.
- Ping Timeout. Enter the ping timeout (how long before the ping test times out) in milliseconds.

Click the **Start Test** button to start the Ping Test.

- Ping Result. The results of the ping test will be shown here.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. Click **Help** for more information.



Figure 5-43: Diagnostics

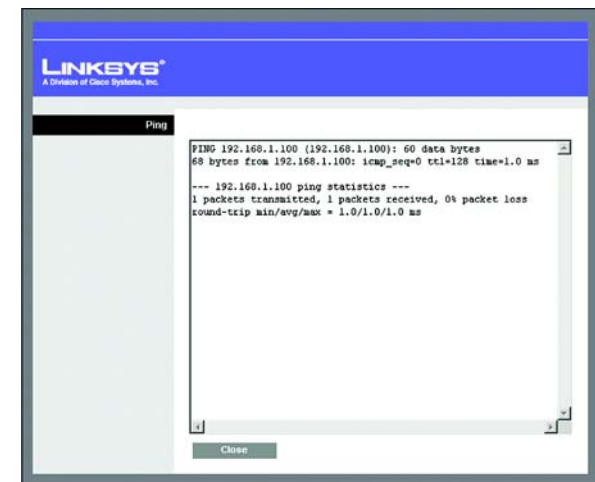


Figure 5-44: Ping Test

## The Backup & Restore Tab

The Backup & Restore tab allows you to back up and restore the Gateway's configuration file.

### Backup Configuration

To back up the Gateway's configuration file, click the **Backup** button. Then follow the on-screen instructions.

### Restore Configuration

To restore the Gateway's configuration file, click the **Browse** button. Then follow the on-screen instructions to locate the file. After you have selected the file, click the **Restore** button.

Click **Help** for more information.



Figure 5-45: Backup & Restore

## The Factory Defaults Tab

If you want to restore the Gateway's factory default settings, then use this screen.

### Factory Defaults

Restore Factory Defaults. If you wish to restore the Gateway to its factory default settings and lose all your settings, click **Restore Factory Defaults**. Then follow the on-screen instructions. Click **Help** for more information.

## The Firmware Upgrade Tab

Use this screen to upgrade the Gateway's firmware.

### Firmware Upgrade

To upgrade the Gateway's firmware:

1. Download the Gateway's firmware upgrade file from [www.linksys.com/international](http://www.linksys.com/international).
2. Extract the file on your computer.
3. On the *Firmware Upgrade* screen, click the **Browse** button to find the firmware upgrade file.
4. Double-click the firmware file that you have downloaded and extracted.
5. Click the **Start to Upgrade** button, and follow the on-screen instructions.

Click **Help** for more information.

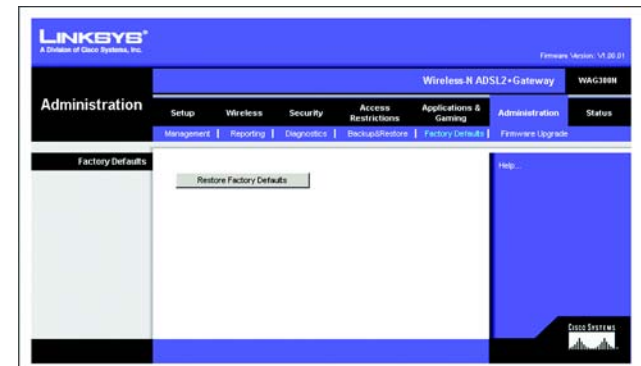


Figure 5-46: Factory Defaults

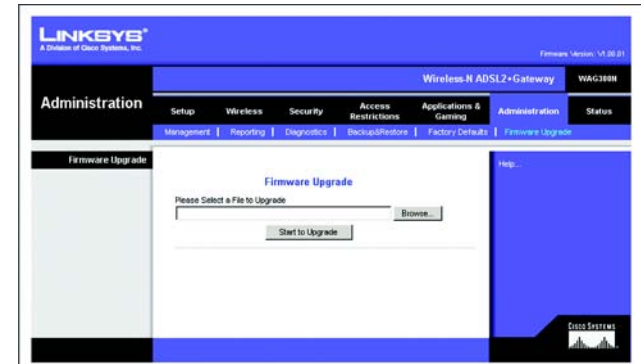


Figure 5-47: Firmware Upgrade

## The Status Tab

### The Gateway Tab

This screen displays information about the Gateway and its Internet connection.

#### Gateway Information

This section displays the Gateway's Firmware Version, MAC Address, and Current Time.

#### Internet Connection

This section shows the following information: Login Type, Interface, IP Address, Subnet Mask, Default Gateway, and DNS 1, 2, and 3 server IP addresses.

**DHCP Renew.** If available, click the **DHCP Renew** button to replace the Gateway's current IP address with a new IP address.

**DHCP Release.** If available, click the **DHCP Release** button to delete the Gateway's current IP address.

Click the **Refresh** button if you want to refresh the displayed information. Click **Help** for more information.



Figure 5-48: Gateway

## The Local Network Tab

This screen displays information about the Gateway's local network.

### Local Network

This screen displays the following: the local Mac Address, IP Address, Subnet Mask, DHCP Server, Start IP Address, and End IP Address.

To view the DHCP Client Table, click the **DHCP Client Table** button. To view the ARP/RARP Table, click the **ARP/RARP Table** button.

**DHCP Clients Table.** The DHCP Active IP Table shows the current DHCP Client data. You will see the computer name, IP address, MAC address, and expiration time of the dynamic IP address for the clients using the DHCP server. (This data is stored in temporary memory and changes periodically.) Click the **Refresh** button if you want to refresh the displayed information. To delete a client from the DHCP server, select the client, and then click the **Delete** button. Click the **Close** button to return to the *Local Network* screen.

**ARP/RARP Table.** An ARP request is a request sent by the Gateway asking clients with IP addresses for their MAC addresses, so the Gateway can map IP addresses to MAC addresses. RARP is the reverse of ARP. The ARP/RARP Table shows the current data for the local network clients of the Gateway. You will see their IP addresses and MAC addresses. (This data is stored in temporary memory and changes periodically.) Click the **Refresh** button if you want to refresh the displayed information. Click the **Close** button to return to the *Local Network* screen.

Click the **Refresh** button if you want to refresh the displayed information. Click **Help** for more information.

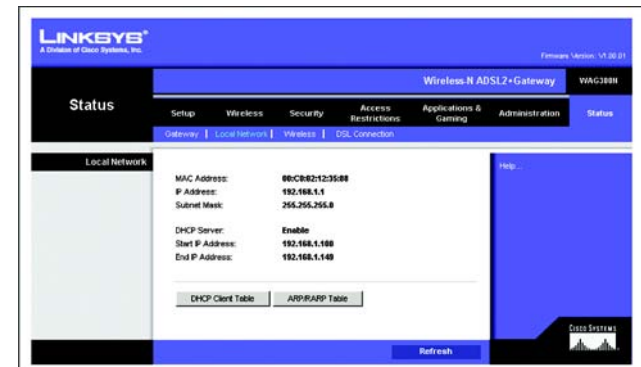


Figure 5-49: Local Network

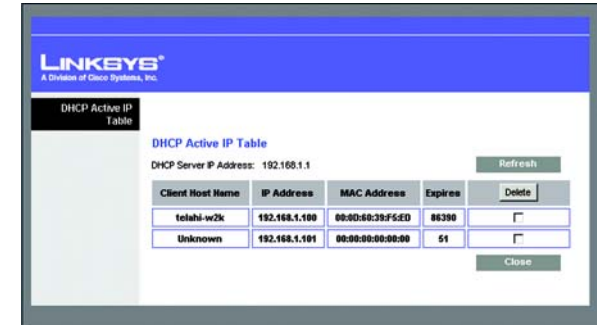


Figure 5-50: DHCP Active IP Table

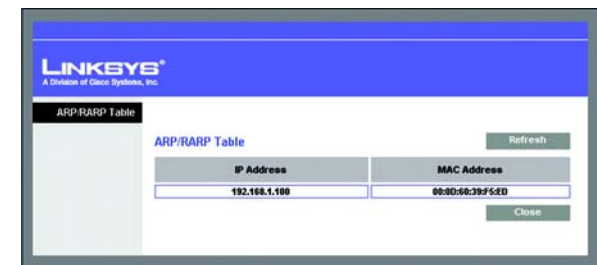


Figure 5-51: ARP/RARP Table

## The Wireless Tab

This screen displays information about the Gateway's wireless network.

### Wireless Network

This screen displays the following: MAC Address, Mode, Network Name (SSID), Radio Band, Wide Channel, Standard Channel, Security method, and SSID Broadcast status.

Click the **Refresh** button if you want to refresh the displayed information. Click **Help** for more information.



Figure 5-52: Wireless

## The DSL Connection Tab

This screen shows information about the DSL connection.

### DSL Status

This section shows the following: Status, Downstream Rate, and Upstream Rate.

### PVC Connection

This section displays the following information: Encapsulation, Multiplexing, QoS, Pcr Rate, Scr Rate, Autodetect, VPI, VCI, Enable status, and PVC Status.

Click the **Refresh** button if you want to refresh the displayed information. Click **Help** for more information.



Figure 5-53: DSL Connection

# Appendix A: Troubleshooting

This appendix consists of two parts: “Common Problems and Solutions” and “Frequently Asked Questions.” Provided are possible solutions to problems that may occur during the installation and operation of the Gateway. Read the descriptions below to help you solve your problems. If you can’t find an answer here, check the Linksys international website at [www.linksys.com](http://www.linksys.com).

## Common Problems and Solutions

### 1. *I need to set a static IP address on a computer.*

You can assign a static IP address to a computer by performing the following steps:

- For Windows 98 and Me:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
  2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the Properties button.
  3. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway. Make sure that each IP address is unique for each computer or network device.
  4. Click the **Gateway** tab, and in the New Gateway prompt, enter 192.168.1.1, which is the default IP address of the Gateway. Click the Add button to accept the entry.
  5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
  6. Click the **OK** button in the TCP/IP properties window, and click **Close** or the **OK** button for the Network window.
  7. Restart the computer when asked.
- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
  3. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
  5. Enter the Subnet Mask, 255.255.255.0.
  6. Enter the Default Gateway, 192.168.1.1 (Gateway’s default IP address).



7. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
  9. Restart the computer if asked.
- For Windows XP:  
The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.
    1. Click **Start** and **Control Panel**.
    2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
    3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the Properties option.
    4. In the **This connection uses the following items** box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
    5. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
    6. Enter the Subnet Mask, 255.255.255.0.
    7. Enter the Default Gateway, 192.168.1.1 (Gateway's default IP address).
    8. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
    9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

**2. I want to test my Internet connection.**

A. Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

- Refer to Windows Help for details. Make sure Obtain IP address automatically is selected in the settings.

For Windows NT 4.0:

- Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
- Click the Protocol tab, and double-click on TCP/IP Protocol.
- When the window appears, make sure you have selected the correct Adapter for your Ethernet adapter and set it for **Obtain an IP address** from a DHCP server.
- Click the **OK** button in the TCP/IP Protocol Properties window, and click the **Close** button in the Network window.
- Restart the computer if asked.

B. Open a command prompt.

For Windows 98 and Me:

- Click **Start** and **Run**. In the Open field, type in command. Press the **Enter** key or click the **OK** button.

For Windows NT, 2000, and XP:

- Click **Start** and **Run**. In the Open field, type cmd. Press the **Enter** key or click the **OK** button. In the command prompt, type ping 192.168.1.1 and press the Enter key.
  - If you get a reply, the computer is communicating with the Gateway.
  - If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.
- C. In the command prompt, type ping followed by your Internet or WAN IP address and press the **Enter** key. The Internet or WAN IP Address can be found on the Status screen of the Gateway's Web-based Utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter ping 1.2.3.4 and press the Enter key.
- If you get a reply, the computer is connected to the Gateway.
  - If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- D. In the command prompt, type ping www.yahoo.com and press the **Enter** key.
- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
  - If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

**3. I am not getting an IP address on the Internet with my Internet connection.**

- Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
  1. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA, Bridged Mode Only, or IPoA. Please refer to the Setup section of "Chapter 5: Configuring the Wireless-N ADSL2+ Gateway" for details on Internet connection settings.
  2. Make sure you have the right cable. Check to see if the Gateway column has a solidly lit ADSL LED.
  3. Make sure the cable connecting from your Gateway's DSL port is connected to the wall jack of the ADSL service line. Verify that the Status page of the Gateway's Web-based Utility shows a valid IP address from your ISP.
  4. Turn off the computer and Gateway. Wait 30 seconds, and then turn on the Gateway, and computer. Check the Status tab of the Gateway's Web-based Utility to see if you get an IP address.

**4. I am not able to access the Setup page of the Gateway's Web-based Utility.**

- Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Gateway.
  1. Refer to "Appendix C: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
  2. Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."

3. Refer to “Problem #10: I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.”

**5. I can't get my Virtual Private Network (VPN) working through the Gateway.**

Access the Gateway's web interface by going to <http://192.168.1.1> or the IP address of the Gateway, and go to the Security tab. Make sure you have IPsec passthrough and/or PPTP pass-through enabled.

- VPNs that use IPsec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPsec session will work through the Gateway; however, simultaneous IPsec sessions may be possible, depending on the specifics of your VPNs.
- VPNs that use IPsec and AH (Authentication Header known as protocol 51) are incompatible with the Gateway. AH has limitations due to occasional incompatibility with the NAT standard.
- Change the IP address for the Gateway to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Gateway will have difficulties routing information to the right location. If you change the Gateway's IP address to 192.168.2.1, that should solve the problem. Change the Gateway's IP address through the Setup tab of the web interface.
- If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.
- Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPsec server. Refer to “Problem #7, I need to set up online game hosting or use other Internet applications” for details.
- Check the Linksys international website for more information at [www.linksys.com](http://www.linksys.com).

**6. I need to set up a server behind my Gateway and make it available to the public.**

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed.

- Follow these steps to set up port forwarding through the Gateway's Web-based Utility. We will be setting up web, ftp, and mail servers.
  1. Access the Gateway's Web-based Utility by going to <http://192.168.1.1> or the IP address of the Gateway. Go to the Applications and Gaming => Port Range Forwarding tab.
  2. Enter any name you want to use for the Application.
  3. Enter the port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
  4. Select the protocol you will be using, TCP and/or UDP.
  5. Enter the IP address of the computer or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the

field provided. Check “Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter” for details on getting an IP address.

6. Check the **Enable** option for the port services you want to use. Consider the example below:

Application	Start and End	Protocol	IP Address	Enable
Web server	80 to 80	Both	192.168.1.100	X
FTP server	21 to 21	TCP	192.168.1.101	X
SMTP (outgoing)	25 to 25	Both	192.168.1.102	X
POP3 (incoming)	110 to 110	Both	192.168.1.102	X

When you have completed the configuration, click the **Save Settings** button.

### 7. *I need to set up online game hosting or use other Internet applications.*

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Gateway to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

1. Access the Gateway’s web interface by going to <http://192.168.1.1> or the IP address of the Gateway. Go to the Applications and Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the Application.
3. Enter the port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Select the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the computer or network device that you want the port server to go to. For example, if the web server’s Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check “Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter” for details on getting an IP address.
6. Check the **Enable** option for the port services you want to use. Consider the example below:

Application	Start and End	Protocol	IP Address	Enable
UT	7777 to 27900	Both	192.168.1.100	X
Half-life	27015 to 27015	Both	192.168.1.105	X

Application	Start and End	Protocol	IP Address	Enable
PC Anywhere	5631 to 5631	UDP	192.168.1.102	X
VPN IPSEC	500 to 500	UDP	192.168.1.100	X

When you have completed the configuration, click the **Save Settings** button.

### **8. I can't get the Internet game, server, or application to work.**

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one computer to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Gateway will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Gateway will send the data to whichever computer or network device you set for DMZ hosting.)

- Follow these steps to set DMZ hosting:
  1. Access the Gateway's Web-based Utility by going to <http://192.168.1.1> or the IP address of the Gateway. Go to the Applications and Gaming => DMZ tab. Click **Enable** and enter the IP address of the computer.
  2. Check the Port Forwarding pages and disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
- Once completed with the configuration, click the **Save Settings** button.

### **9. I forgot my password, or the password prompt always appears when I am saving settings to the Gateway.**

- Reset the Gateway to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:
  1. Access the Gateway's Web-based Utility by going to <http://192.168.1.1> or the IP address of the Gateway. Enter the default username and password **admin**, and click the **Administrations => Management** tab.
  2. Enter a different password in the *Gateway Password* field, and enter the same password in the second field to confirm the password.
  3. Click the **Save Settings** button.

### **10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.**

If you have proxy settings, you need to disable these on your computer. Because the Gateway is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

- For Microsoft Internet Explorer 5.0 or higher:
  1. Click **Start, Settings, and Control Panel**. Double-click Internet Options.
  2. Click the **Connections** tab.
  3. Click the **LAN settings** button and remove anything that is checked.
  4. Click the **OK** button to go back to the previous screen.
  5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.
- For Netscape 6 or higher:
  1. Start **Netscape Navigator**, and click **Edit, Preferences, Advanced, and Proxies**.
  2. Make sure you have Direct connection to the Internet selected on this screen.
  3. Close all the windows to finish.

**11. To start over, I need to set the Gateway to factory default.**

Hold the **Reset** button for 10 seconds and then release it. This will return the Internet settings, password, forwarding, and other settings on the Gateway to the factory default settings. In other words, the Gateway will revert to its original factory configuration.

**12. I need to upgrade the firmware.**

In order to upgrade the firmware with the latest features, you need to go to the Linksys international website and download the latest firmware at [www.linksys.com/international](http://www.linksys.com/international).

- Follow these steps:
  1. Go to the Linksys international website at <http://www.linksys.com> and select your region or country.
  2. Click the **Products** tab and select the Gateway.
  3. On the Gateway's webpage, click **Firmware**, and then download the latest firmware for the Gateway.
  4. To upgrade the firmware, follow the steps in the Administration section found in "Chapter 5: Configuring the Wireless-N ADSL2+ Gateway."

**13. The firmware upgrade failed, and/or the Power LED is flashing.**

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Power LED stop flashing:

- If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- Set a static IP address on the computer; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:  
IP Address: 192.168.1.50  
Subnet Mask: 255.255.255.0  
Gateway: 192.168.1.1

- Perform the upgrade using the TFTP program or the Gateway's Web-based Utility through its Administration tab.

**14. My DSL service's PPPoE is always disconnecting.**

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet.

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.
  1. To connect to the Gateway, go to the web browser, and enter `http://192.168.1.1` or the IP address of the Gateway.
  2. Enter the username and password, if asked. (The default username and password is admin.)
  3. On the *Setup* screen, select the option **Keep Alive**, and set the Redial Period option to **30** (seconds) (this will keep the connection to the ISP and will not disconnect).
  4. Click the **Save Settings** button. Click the **Status** tab, and click the **Connect** button.
  5. You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
  6. Click the **Save Settings** button to continue.
- If the connection is lost again, follow steps 1- 6 to re-establish connection.

**15. I can't access my e-mail, web, or VPN, or I am getting corrupted data from the Internet.**

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set automatically.

- If you are having some difficulties, perform the following steps:
  1. To connect to the Gateway, go to the web browser, and enter `http://192.168.1.1` or the IP address of the Gateway.
  2. Enter the username and password, if asked. (The default username and password is admin.)
  3. Look for the MTU option, and select **Manual**. In the *Size* field, enter **1492**.
  4. Click the **Save Settings** button to continue.
- If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
  - 1462
  - 1400
  - 1362
  - 1300

**16. The Power LED flashes continuously.**

The Power LED lights up when the device is first powered up. In the meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED remains steady to show that the system is working fine. If the LED continues to flash after this time, the device is not working properly. Try

to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0.

**17. When I enter a URL or IP address, I get a time-out error or am prompted to retry.**

- Check if other computers work. If they do, ensure that your computer's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the computers are configured correctly, but still not working, check the Gateway. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Gateway is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Gateway to verify a direct connection.
- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools, Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit, Preferences, Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

**18. I'm trying to access the Gateway's Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, "404 Forbidden."**

If you are using Windows Explorer, perform the following steps until you see the Web-based Utility's login screen (Netscape Navigator will require similar steps):

1. Click **File**. Make sure *Work Offline* is NOT checked.
  2. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.
- Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

## Frequently Asked Questions

***What is the maximum number of IP addresses that the Gateway will support?***

The Gateway will support up to 253 IP addresses.

***Is IPSec Passthrough supported by the Gateway?***

Yes, it is a built-in feature that is enabled by default.

***Where is the Gateway installed on the network?***

In a typical environment, the Gateway is installed between the ADSL wall jack and the LAN.



***Does the Gateway support IPX or AppleTalk?***

No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to a LAN.

***Does the LAN connection of the Gateway support 100Mbps Ethernet?***

The Gateway supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Gateway.

***What is Network Address Translation and what is it used for?***

Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a computer connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Gateway to be used with low cost Internet accounts when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

***Does the Gateway support any operating system other than Windows 98SE, Windows Millennium, Windows 2000, or Windows XP?***

Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

***Does the Gateway support ICQ send file?***

Yes, with the following fix: click ICQ menu -> preference -> connections tab->, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the Gateway.

***I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?***

If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Gateway from your ISP.

***Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?***

It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

***How do I get Half-Life: Team Fortress to work with the Gateway?***

The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

***The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?***

Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at [www.linksys.com](http://www.linksys.com) for more information.

***If all else fails in the installation, what can I do?***

Reset the Gateway by holding down the reset button until the Power LED fully turns on and off. Reset your DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys international website, [www.linksys.com](http://www.linksys.com).

***How will I be notified of new Gateway firmware upgrades?***

All Linksys firmware upgrades are posted on the Linksys international website at [www.linksys.com](http://www.linksys.com), where they can be downloaded for free. To upgrade the Gateway's firmware, use the Administration tab of the Gateway's Web-based Utility. If the Gateway's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use.

***Will the Gateway function in a Macintosh environment?***

Yes, but the Gateway's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

***I am not able to get the web configuration screen for the Gateway. What can I do?***

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

***What is DMZ Hosting?***

Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you

## Wireless-N ADSL2+ Gateway

want to use DMZ Hosting. To get the LAN IP address, see “Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter.”

***If DMZ Hosting is used, does the exposed user share the public IP with the Gateway?***

No.

***Does the Gateway pass PPTP packets or actively route PPTP sessions?***

The Gateway allows PPTP packets to pass through.

***Is the Gateway cross-platform compatible?***

Any platform that supports Ethernet and TCP/IP is compatible with the Gateway.

***How many ports can be simultaneously forwarded?***

Theoretically, the Gateway can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

***What are the advanced features of the Gateway?***

The Gateway’s advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing, and DDNS.

***How can I check whether I have static or DHCP IP Addresses?***

Consult your ISP to obtain this information.

***How do I get mIRC to work with the Gateway?***

Under the Port Forwarding tab, set port forwarding to 113 for the computer on which you are using mIRC.

***Can the Gateway act as my DHCP server?***

Yes. The Gateway has DHCP server software built-in.

***Can I run an application from a remote computer over the wireless network?***

This will depend on whether or not the application is designed to be used over a network. Consult the application’s documentation to determine if it supports operation over a network.

***What is the IEEE 802.11g standard?***

It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

***What is the IEEE 802.11b standard?***

It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

***What IEEE 802.11b and 802.11g features are supported?***

The product supports the following IEEE 802.11b and IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

It also supports OFDM technology for 802.11g networking.

***What is ad-hoc mode?***

When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other, peer-to-peer without the use of an access point.

***What is infrastructure mode?***

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a network through a wireless access point.

***What is roaming?***

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the computer must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives

acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

### ***What is the ISM band?***

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

### ***What is Spread Spectrum?***

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

### ***What is DSSS? What is FHSS? And what are their differences?***

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

### ***Will the information be intercepted while it is being transmitted through the air?***

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

### ***What is WEP?***

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

### ***What is a MAC Address?***

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all

## Wireless-N ADSL2+ Gateway

practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

### ***How do I reset the Gateway?***

Press the Reset button on the back panel for about ten seconds. This will reset the Gateway to its default settings.

### ***How do I resolve issues with signal loss?***

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Gateway and a wireless computer will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Gateway and your wireless computer in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel.

### ***I have excellent signal strength, but I cannot see my network.***

Wireless security is probably enabled on the Gateway, but not on your wireless adapter (or vice versa). Verify that the same wireless security settings are being used on all devices of your wireless network.

### ***How many channels/frequencies are available with the Gateway?***

There are eleven available channels, ranging from 1 to 11, in most of North, Central, and South America. There are thirteen available channels, ranging from 1 to 13, in most of Europe. There may be additional channels available in other regions, subject to the regulations of your region and/or country.

If your questions are not addressed here, refer to the Linksys website, [www.linksys.com](http://www.linksys.com).

# Appendix B: Wireless Security

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

## Security Precautions

The following is a complete list of security precautions to take (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use PSK if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

For information on implementing these security features, refer to “Chapter 5: Configuring the Wireless-N ADSL2+ Gateway.”

## Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for “beacon messages”. These messages can be easily decrypted and contain much of the network’s information, such as the network’s SSID (Service Set Identifier). Here are the steps you can take:

**Change the administrator’s password regularly.** With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator’s password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator’s password regularly.



**NOTE:** Some of these security features are available only through the network gateway, router, or access point. Refer to the gateway, router, or access point’s documentation for more information.

**SSID.** There are several things to keep in mind about the SSID:

1. Disable Broadcast
2. Make it unique
3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

**MAC Addresses.** Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

**WEP Encryption.** Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible
2. Use "Shared Key" authentication
3. Change your WEP key regularly

**PSK.** Pre-Shared Key (PSK) is the newest and best available standard in Wi-Fi security. **PSK2** is the newer version of Pre-Shared Key with stronger encryption than PSK. PSK gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. PSK-Enterprise and PSK2-Enterprise use a RADIUS (Remote Authentication Dial-In User Service) server for authentication. RADIUS uses a RADIUS server and WEP encryption.



**IMPORTANT:** Always remember that each device in your wireless network **MUST** use the same encryption method and encryption key or your wireless network will not function properly.



**PSK-Personal.** Select the type of algorithm, TKIP or AES, enter a password in the Passphrase field of 8-63 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Gateway or other device how often it should change the encryption keys.

**PSK2-Personal.** PSK2 gives you one encryption method, AES, with dynamic encryption keys. Enter a Passphrase of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Gateway how often it should change the encryption keys.

**PSK-Enterprise.** This method is PSK used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Gateway and its RADIUS server. Then enter a Key Renewal Timeout period, which instructs the Gateway how often it should change the encryption keys.

**PSK2-Enterprise.** This method is PSK2 used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Gateway and its RADIUS server. Then enter a Key Renewal Timeout period, which instructs the Gateway how often it should change the encryption keys.

**RADIUS.** This method is WEP used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Gateway and its RADIUS server. Enter the WEP settings.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

# Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering feature of the Gateway. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Gateway's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

## Windows 98 or Me Instructions

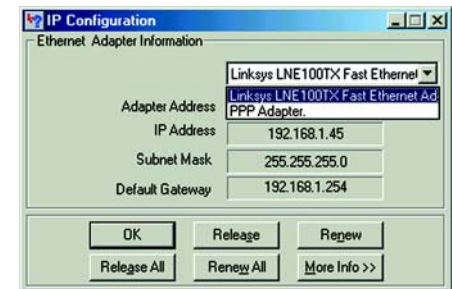
1. Click **Start** and **Run**. In the *Open* field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.
2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Gateway via a CAT 5 Ethernet network cable. See Figure C-1.
3. Write down the Adapter Address as shown on your computer screen (see Figure C-2). This is the MAC address for your Ethernet adapter and is shown in hexadecimal as a series of numbers and letters.

The MAC address/Adapter Address is what you will use for MAC filtering. The example in Figure D-2 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

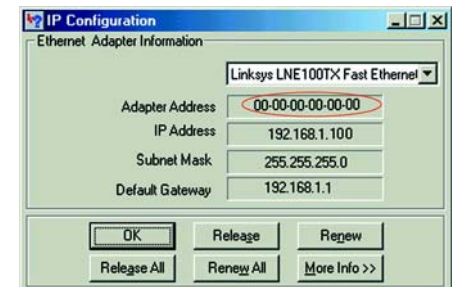
The example in Figure C-2 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.



**NOTE:** The MAC address is also called the Adapter Address.



**Figure C-1: IP Configuration Screen**



**Figure C-2: MAC Address/Adapter Address**

## Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.

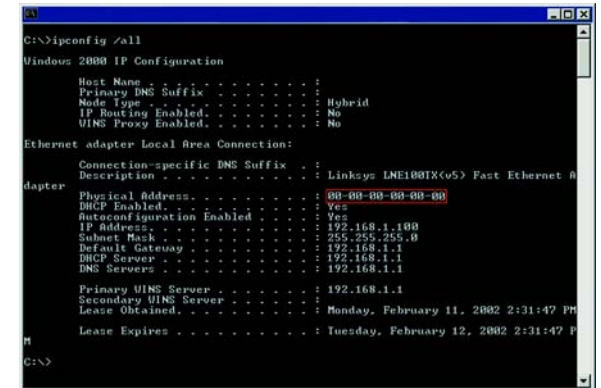


**NOTE:** The MAC address is also called the Physical Address.

2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.
3. Write down the Physical Address as shown on your computer screen (Figure C-3); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

The MAC address/Physical Address is what you will use for MAC filtering. The example in Figure C-3 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

The example in Figure C-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.



```
C:\>ipconfig /all

Windows 2000 IP Configuration

Host Name . . . . . :
Primary DNS Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  :
   Description . . . . . : Linksys LNE100TX(v5) Fast Ethernet A
dapter
   Physical Address. . . . . : 00-00-00-00-00-00
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address. . . . . : 192.168.1.100
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.1.1
   DHCP Server . . . . . : 192.168.1.1
   DNS Servers . . . . . : 192.168.1.1
   Primary WINS Server . . . . . : 192.168.1.1
   Secondary WINS Server . . . . . :
   Lease Obtained. . . . . : Monday, February 11, 2002 2:31:47 PM
   Lease Expires . . . . . : Tuesday, February 12, 2002 2:31:47 PM

C:\>
```

**Figure C-3: MAC Address/Physical Address**

# Appendix D: Upgrading Firmware

To upgrade the Gateway's firmware:

1. Download the Gateway's firmware upgrade file from *www.linksys.com/international*.
2. Extract the file on your computer.
3. Open the Gateway's Web-based Utility and click the **Administration** tab.
4. Click the **Firmware Upgrade** tab.
5. Click the **Browse** button to find the extracted file, and then double-click it.
6. Click the **Upgrade** button, and follow the on-screen instructions.

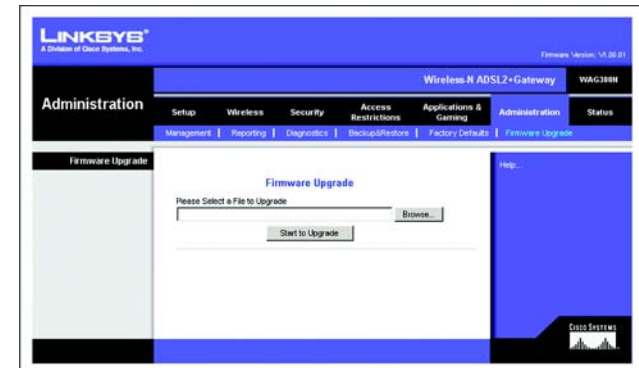


Figure D-1: Firmware Upgrade

# Appendix E: Glossary

This glossary contains some basic networking terms you may come across when using this product. For more advanced terms, see the complete Linksys glossary at <http://www.linksys.com/glossary>.

**Access Point** - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

**Ad-hoc** - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

**AES (Advanced Encryption Standard)** - A security method that uses symmetric 128-bit block data encryption.

**Bandwidth** - The transmission capacity of a given device or network.

**Bit** - A binary digit.

**Boot** - To start a device and cause it to start executing instructions.

**Broadband** - An always-on, fast Internet connection.

**Browser** - An application program that provides a way to look at and interact with all the information on the World Wide Web.

**Byte** - A unit of data that is usually eight bits long.

**Cable Modem** - A device that connects a computer to the cable television network, which in turn connects to the Internet.

**Daisy Chain** - A method used to connect devices in a series, one after the other.

**DDNS (Dynamic Domain Name System)** - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., [www.xyz.com](http://www.xyz.com)) and a dynamic IP address.

**Default Gateway** - A device that forwards Internet traffic from your local area network.

**DHCP (Dynamic Host Configuration Protocol)** - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

## Wireless-N ADSL2+ Gateway

**DMZ (Demilitarized Zone)** - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

**DNS (Domain Name Server)** - The IP address of your ISP's server, which translates the names of websites into IP addresses.

**Domain** - A specific name for a network of computers.

**Download** - To receive a file transmitted over a network.

**DSL (Digital Subscriber Line)** - An always-on broadband connection over traditional phone lines.

**Dynamic IP Address** - A temporary IP address assigned by a DHCP server.

**EAP (Extensible Authentication Protocol)** - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

**Encryption** - Encoding data transmitted in a network.

**Ethernet** - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

**Firewall** - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

**Firmware** - The programming code that runs a networking device.

**FTP (File Transfer Protocol)** - A protocol used to transfer files over a TCP/IP network.

**Full Duplex** - The ability of a networking device to receive and transmit data simultaneously.

**Gateway** - A device that interconnects networks with different, incompatible communications protocols.

**Half Duplex** - Data transmission that can occur in two directions over a single line, but only one direction at a time.

**HTTP (HyperText Transport Protocol)** - The communications protocol used to connect to servers on the World Wide Web.

**Infrastructure** - A wireless network that is bridged to a wired network via an access point.

**IP (Internet Protocol)** - A protocol used to send data over a network.

**IP Address** - The address used to identify a computer or device on a network.

**IPCONFIG** - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

**IPSec (Internet Protocol Security)** - A VPN protocol used to implement secure exchange of packets at the IP layer.

**ISP (Internet Service Provider)** - A company that provides access to the Internet.

**LAN** - The computers and networking products that make up your local network.

**MAC (Media Access Control) Address** - The unique address that a manufacturer assigns to each networking device.

**Mbps (MegaBits Per Second)** - One million bits per second; a unit of measurement for data transmission.

**NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

**Network** - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

**Packet** - A unit of data sent over a network.

**Passphrase** - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

**Ping (Packet Internet Groper)** - An Internet utility used to determine whether a particular IP address is online.

**POP3 (Post Office Protocol 3)** - A standard mail server commonly used on the Internet.

**Port** - The connection point on a computer or networking device used for plugging in cables or adapters.

**Power over Ethernet (PoE)** - A technology enabling an Ethernet network cable to deliver both data and power.

**PPPoE (Point to Point Protocol over Ethernet)** - A type of broadband connection that provides authentication (username and password) in addition to data transport.

**PPTP (Point-to-Point Tunneling Protocol)** - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

**RADIUS (Remote Authentication Dial-In User Service)** - A protocol that uses an authentication server to control network access.

## Wireless-N ADSL2+ Gateway

**RJ-45 (Registered Jack-45)** - An Ethernet connector that holds up to eight wires.

**Roaming** - The ability to take a wireless device from one access point's range to another without losing the connection.

**Router** - A networking device that connects multiple networks together.

**Server** - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

**SMTP (Simple Mail Transfer Protocol)** - The standard e-mail protocol on the Internet.

**SNMP (Simple Network Management Protocol)** - A widely used network monitoring and control protocol.

**SPI (Stateful Packet Inspection) Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

**SSID (Service Set Identifier)** - Your wireless network's name.

**Static IP Address** - A fixed address assigned to a computer or device that is connected to a network.

**Static Routing** - Forwarding data in a network via a fixed path.

**Subnet Mask** - An address code that determines the size of the network.

**Switch** - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

**TCP (Transmission Control Protocol)** - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** - A set of instructions PCs use to communicate over a network.

**Telnet** - A user command and TCP/IP protocol used for accessing remote PCs.

**TFTP (Trivial File Transfer Protocol)** - A version of the TCP/IP FTP protocol that has no directory or password capability.

**Throughput** - The amount of data moved successfully from one node to another in a given time period.



## Wireless-N ADSL2+ Gateway

**TKIP (Temporal Key Integrity Protocol)** - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

**Topology** - The physical layout of a network.

**TX Rate** - Transmission Rate.

**Upgrade** - To replace existing software or firmware with a newer version.

**Upload** - To transmit a file over a network.

**URL (Uniform Resource Locator)** - The address of a file located on the Internet.

**VPN (Virtual Private Network)** - A security measure to protect data as it leaves one network and goes to another over the Internet.

**WAN (Wide Area Network)**- The Internet.

**WEP (Wired Equivalent Privacy)** - A method of encrypting network data transmitted on a wireless network for greater security.

**WLAN (Wireless Local Area Network)** - A group of computers and associated devices that communicate with each other wirelessly.

**WPA (Wi-Fi Protected Access)** - A wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

# Appendix F: Specifications

<b>Model Number</b>	<b>WAG300N</b>
<b>Standards</b>	<b>Draft 802.11N, IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, IEEE 802.3, g.992.1 (g.dmt), g.992.2 (g.lite), g.992.3, g.992.5, T1.413i2, Annex B (WAG300N-EU), UR-2 Deutsche Telekom (WAG300N-DE)</b>
<b>Ports</b>	<b>Power, DSL, Ethernet (1-4)</b>
<b>Button</b>	<b>Reset, Power</b>
<b>Cabling Type</b>	<b>CAT 5 UTP</b>
<b>LEDs</b>	<b>Power, Wireless, Ethernet (1-4), DSL, Internet</b>
<b>Number of Antennas</b>	<b>3</b>
<b>Connector Type</b>	<b>Fixed</b>
<b>Detachable (yes/no)</b>	<b>no</b>
<b>RF Pwr (EIRP) in dBm</b>	<b>17</b>
<b>Antenna Gain in dBi</b>	<b>2</b>
<b>UPnP able/cert</b>	<b>Able</b>

## Wireless-N ADSL2+ Gateway

<b>Security Features</b>	Password protected configuration for web access PAP and CHAP authentication Denial of Service (DoS) Prevention URL filtering, and keyword, Java, ActiveX, Proxy, Cookie blocking ToD filter (Blocks Access by Time VPN Passthrough for IPSec, PPTP, and L2TP Protocols 128, 64 bits WEP with Passphrase WEP key generation SSID Broadcast Disable Access restriction by MAC and IP addresses
<b>WEP Key Bits</b>	64, 128
<b>Dimensions</b>	140 mm x 140 mm x 27 mm
<b>Unit Weight</b>	0.27 kg
<b>Power</b>	12VDC, 1A
<b>Certifications</b>	CE
<b>Operating Temp.</b>	0° to 40°C
<b>Storage Temp.</b>	-20° to 70°C
<b>Operating Humidity</b>	10 to 85% Non-Condensing
<b>Storage Humidity</b>	5 to 90% Non-Condensing

**Note:** Actual broadband speeds are dependent on the ISP, wireless security, and other factors.

# Appendix G: Warranty Information

Linksys warrants to You that, for a period of three years (the "Warranty Period"), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

**This Warranty is valid and may be processed only in the country of purchase.**

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

# Appendix H: Regulatory Information

## FCC Statement

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

## FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

## Safety Notices

Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.

Do not use this product near water, for example, in a wet basement or near a swimming pool.

Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

## Industry Canada (Canada)

This device complies with Industry Canada ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB003 et RSS210 d'Industrie Canada.

## **Dual-Band Wireless Access Point**

### **IC Statement**

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

### **Règlement d'Industry Canada**

Le fonctionnement est soumis aux conditions suivantes :

1. Ce périphérique ne doit pas causer d'interférences;
2. Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable.

## Wireless-N ADSL2+ Gateway

### Compliance Information for 2.4-GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

### Declaration of Conformity with Regard to the EU Directive 1999/5/EC (R&TTE Directive)

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιαστικές απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Română [Romanian]:	Acest echipament este în conformitate cu cerințele esențiale și cu alte prevederi relevante ale Directivei 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

**NOTE:** For all products, the Declaration of Conformity is available through one or more of these options:

- A pdf file is included on the product's CD.
- A print copy is included with the product.
- A pdf file is available on the product's webpage. Visit [www.linksys.com/international](http://www.linksys.com/international) and select your country or region. Then select your product.

If you need any other technical documentation, see the "Technical Documents on [www.linksys.com/international](http://www.linksys.com/international)" section, as shown later in this appendix.

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 300 328
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950 and either EN 50385 or EN 50371

#### CE Marking

For the Linksys Wireless-B and Wireless-G products, the following CE mark, notified body number (where applicable), and class 2 identifier are added to the equipment.



Check the CE label on the product to find out which notified body was involved during the assessment.

#### National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

*Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:*

*Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:*

*Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1999/5/CE folgen) mit Ausnahme der folgenden aufgeführten Staaten:*



## Wireless-N ADSL2+ Gateway

### Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <http://www.bipt.be> for more details.

*Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <http://www.bipt.be> voor meer gegevens.*

*Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <http://www.ibpt.be> pour de plus amples détails.*

### France

In case the product is used outdoors, the output power is restricted in some parts of the band. See Table 1 or check <http://www.arcep.fr/> for more details.

*Dans la cas d'une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous à la table 1 ou visitez <http://www.arcep.fr/> pour de plus amples détails.*

Table 1: Applicable Power Levels in France

Location	Frequency Range (MHz)	Power (EIRP)
Indoor (No restrictions)	2400-2483.5	100 mW (20 dBm)
Outdoor	2400-2454 2454-2483.5	100 mW (20 dBm) 10 mW (10 dBm)

### Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless operating within the boundaries of the owner's property, the use of this 2.4 GHz Wireless LAN product requires a 'general authorization'. Please check with <http://www.comunicazioni.it/it/> for more details.

*Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una "Autorizzazione Generale". Consultare <http://www.comunicazioni.it/it/> per maggiori dettagli.*

## Wireless-N ADSL2+ Gateway

### Product Usage Restrictions

This product is designed for indoor usage only. Outdoor usage is not recommended.

This product is designed for use with the standard, integral or dedicated (external) antenna(s) that is/are shipped together with the equipment. However, some applications may require the antenna(s), if removable, to be separated from the product and installed remotely from the device by using extension cables. For these applications, Linksys offers an R-SMA extension cable (AC9SMA) and an R-TNC extension cable (AC9TNC). Both of these cables are 9 meters long and have a cable loss (attenuation) of 5 dB. To compensate for the attenuation, Linksys also offers higher gain antennas, the HGA7S (with R-SMA connector) and HGA7T (with R-TNC connector). These antennas have a gain of 7 dBi and may only be used with either the R-SMA or R-TNC extension cable.

Combinations of extension cables and antennas resulting in a radiated power level exceeding 100 mW EIRP are illegal.

### Power Output of Your Device

To comply with your country's regulations, you may have to change the power output of your wireless device. Proceed to the appropriate section for your device.

**NOTE:** The power output setting may not be available on all wireless products. For more information, refer to the documentation on your product's CD or <http://www.linksys.com/international>.

### Wireless Adapters

Wireless adapters have the power output set to 100% by default. Maximum power output on each adapter does not exceed 20 dBm (100 mW); it is generally 18 dBm (64 mW) or below. If you need to alter your wireless adapter's power output, follow the appropriate instructions for your computer's Windows operating system:

#### Windows XP

3. Double-click the **Wireless** icon in your desktop's system tray.
4. Open the *Wireless Network Connection* window.
5. Click the **Properties** button.
6. Select the **General** tab, and click the **Configure** button.
7. In the *Properties* window, click the **Advanced** tab.
8. Select **Power Output**.
9. From the pull-down menu on the right, select the wireless adapter's power output percentage.

## Wireless-N ADSL2+ Gateway

### Windows 2000

1. Open the **Control Panel**.
2. Double-click **Network and Dial-Up Connections**.
3. Select your current wireless connection, and select **Properties**.
4. From the *Properties* screen, click the **Configure** button.
5. Click the **Advanced** tab, and select **Power Output**.
6. From the pull-down menu on the right, select the wireless adapter's power setting.

If your computer is running Windows Millennium or 98, then refer to Windows Help for instructions on how to access the advanced settings of a network adapter.

### Wireless Access Points, Routers, or Other Wireless Products

If you have a wireless access point, router or other wireless product, use its Web-based Utility to configure its power output setting (refer to the product's documentation for more information).

### Technical Documents on [www.linksys.com/international](http://www.linksys.com/international)

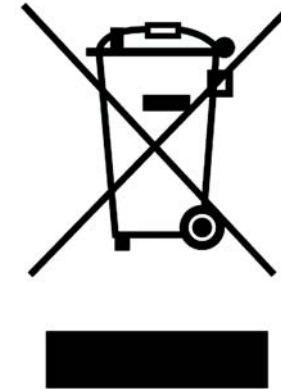
Follow these steps to access technical documents:

1. Enter <http://www.linksys.com/international> in your web browser.
2. Select the country or region in which you live.
3. Click the Products tab.
4. Select the appropriate product category.
5. Select the product sub-category, if necessary.
6. Select the product.
7. Select the type of documentation you want from the More Information section. The document will open in PDF format if you have Adobe Acrobat installed on your computer.

**NOTE:** If you have questions regarding the compliance of these products or you cannot find the information you need, please contact your local sales office or visit <http://www.linksys.com/international> for more details.

**User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)**

This document contains important information for users with regards to the proper disposal and recycling of Linksys products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:



**English**

**Environmental Information for Customers in the European Union**

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

**Ceština/Czech**

**Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie**

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.

## Dansk/Danish

### Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

## Deutsch/German

### Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltsmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

## Eesti/Estonian

### Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

## Español/Spanish

### Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

## Ελληνικά/Greek

### Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινотικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

## Français/French

### Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

## Italiano/Italian

### Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

## Latviešu valoda/Latvian

### Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķīrotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskās un elektroniskās ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojušu aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

## Lietuvškai/Lithuanian

### Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdurbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

## Malti/Maltese

### Informazzjoni Ambjentali għal Kliġenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jstax jintrema ma' skart municiġpali li ma għiex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir iehor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' għbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riciklagg jghin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħha tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-hanut minn fejn xtrajt il-prodott.

## Magyar/Hungarian

### Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyekben, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőrendszeren keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

## Nederlands/Dutch

### Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

## Norsk/Norwegian

### Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

## Polski/Polish

### Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

## Português/Portuguese

### Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através dos instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

## Slovenčina/Slovak

### Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

## Slovenčina/Slovene

### Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjstvih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

## Suomi/Finnish

### Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

## Svenska/Swedish

### Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

For more information, visit [www.linksys.com](http://www.linksys.com).



# Appendix I: Contact Information

Need to contact Linksys?

Visit us online for information on the latest products and updates to your existing products at:  
<http://www.linksys.com/international>

If you experience problems with any Linksys product, you can e-mail us at:

<b>In Europe</b>	<b>E-mail Address</b>
Austria	support.at@linksys.com
Belgium	support.be@linksys.com
Czech Republic	support.cz@linksys.com
Denmark	support.dk@linksys.com
Finland	support.fi@linksys.com
France	support.fr@linksys.com
Germany	support.de@linksys.com
Greece	support.gr@linksys.com (English only)
Hungary	support.hu@linksys.com
Ireland	support.ie@linksys.com
Italy	support.it@linksys.com
Netherlands	support.nl@linksys.com
Norway	support.no@linksys.com
Poland	support.pl@linksys.com
Portugal	support.pt@linksys.com
Russia	support.ru@linksys.com
Spain	support.es@linksys.com
Sweden	support.se@linksys.com

## Wireless-N ADSL2+ Gateway

<b>In Europe</b>	<b>E-mail Address</b>
Switzerland	support.ch@linksys.com
United Kingdom	support.uk@linksys.com

<b>Outside of Europe</b>	<b>E-mail Address</b>
Asia Pacific	asiасupport@linksys.com (English only)
Latin America	support.portuguese@linksys.com or support.spanish@linksys.com
Middle East & Africa	support.mea@linksys.com (English only)
South Africa	support.ze@linksys.com (English only)
UAE	support.ae@linksys.com (English only)
U.S. and Canada	support@linksys.com

Note: For some countries, support may be available only in English.